Calendar No. 1127

93D CONGRESS
2d Session

SENATE

REPORT
No. 93-1183

PROTECTING INDIVIDUAL PRIVACY IN FEDERAL GATHERING, USE AND DISCLOSURE OF INFORMATION

REPORT

OF THE

COMMITTEE ON GOVERNMENT OPERATIONS
UNITED STATES SENATE

TO ACCOMPANY

S. 3418

TO ESTABLISH A PRIVACY PROTECTION COMMISSION, TO PROVIDE MANAGEMENT SYSTEMS IN FEDERAL AGENCIES AND CERTAIN OTHER ORGANIZATIONS WITH RESPECT TO THE GATHERING AND DISCLOSURE OF INFORMATION CONCERNING INDIVIDUALS, AND FOR OTHER PURPOSES

SEPTEMBER 26, 1974.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1974

38-010

CONTENTS

Calendar No. 1127

93D CONGRESS
2d Session

SENATE

REPORT
No. 93-1183

PROTECTING INDIVIDUAL PRIVACY IN FEDERAL GATHERING, USE AND DISCLOSURE OF INFORMATION

SEPTEMBER 26, 1974.—Ordered to be printed

Mr. ERVIN, from the Committee on Government Operations, submitted the following

REPORT

[To accompany S. 3418]

The Committee on Government Operations, to which was referred the bill (S. 3418) to establish a Federal Privacy Board to oversee the gathering and disclosure of information concerning individuals, to provide management systems in Federal agencies, State and local governments, and other organizations regarding such information, and for other purposes, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and an amended title and recommends that the bill as amended do pass.

PURPOSE

The purpose of S. 3418, as amended, is to promote governmental respect for the privacy of citizens by requiring all departments and agencies of the executive branch and their employees to observe certain constitutional rules in the computerization, collection, management, use, and disclosure of personal information about individuals.

It is to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government and with respect to all of its other manual or mechanized files.

It is designed to prevent the kind of illegal, unwise, overbroad, investigation and record surveillance of law-abiding citizens produced in recent years from actions of some over-zealous investigators, and the curiosity of some government administrators, or the wrongful disclosure and use, in some cases, of personal files held by Federal agencies.

It is to prevent the secret gathering of information on people or the creation of secret information systems or data banks on Americans by employees of the departments and agencies of the executive branch.

It is designed to set in motion for long-overdue evaluation of the needs of the Federal Government to acquire and retain personal information on Americans, by requiring stricter review within agencies of criteria for collection and retention.

It is also to promote observance of valued principles of fairness and individual privacy by those who develop, operate, and administer other major institutional and organizational data banks of government and society.

S. 3418 Accomplishes These Purposes in Five Major Ways

First, it requires agencies to give detailed notice of the nature and uses of their personal data banks and information systems and their computer resources. It requires a new Privacy Commission to maintain and publish an information directory for the public, to examine executive branch proposals for new personal data banks and systems, and to report to Congress and the President if they adversely affect privacy and individual rights. It penalizes those who keep secret such a personal information system or data bank.

Second, the bill establishes certain minimum information-gathering standards for all agencies to protect the privacy and due process rights of the individual and to assure that surrender of personal information is made with informed consent or with some guarantees of the uses and confidentiality of the information. To this end, it charges agencies:

To collect, solicit and maintain only personal information that is relevant and necessary for a statutory purpose of the agency;

To prevent hearsay and inaccuracies by collecting information directly from the person involved as far as practicable;

To inform people requested or required to reveal information about themselves whether their disclosure is mandatory or voluntary, what uses and penalties are involved, and what confidentiality guarantees surround the data once government acquires it; and

To establish no program for collecting or maintaining information on how people exercise First Amendment rights without a strict reviewing process.

Third, the bill establishes certain minimum standards for handling and processing personal information maintained in the data banks and systems of the executive branch, for preserving the security of the computerized or manual system, and for safeguarding the confidentiality of the information. To this end, it requires every department and agency to insure, by whatever steps they deem necessary:

That the information they keep, disclose, or circulate about citizens is as accurate, complete, timely, and relevant to the agency's needs as possible;

That they refrain from disclosing it unless necessary for employee duties, or from making it available outside the agency

without the consent of the individual and proper guarantees, unless pursuant to open records laws, or unless it is for certain law enforcement or other purposes;

That they take certain administrative actions to keep account of the employees and people and organizations who have access to the system or file, and to keep account of the disclosures and uses made of the information;

That they establish rules of conduct with regard to theiothical and legal obligations in developing and operating a computerized or other data system and in handling personal data, and take action to instruct all employees of such duties;

That they not sell or rent the names and addresses of people whose files they hold; and

That they issue appropriate administrative orders, provide personnel sanctions, and establish appropriate technical and physical safeguards to insure the security of the information system and the confidentiality of the data.

Fourth, to aid in the enforcement of these legislative restraints, the bill provides administrative and judicial machinery for oversight and for civil remedy of violations. To this end, the bill:

Gives the individual the right, with certain exceptions, to be told upon request whether or not there is a government record on him or her, to have access to it, and to challenge it with a hearing upon request, and with judicial review in Federal Court;

Establishes an independent Privacy Protection Commission with subpoena power and authority to receive and investigate charges of violations of the Act and report them to the proper officials; to develop model guidelines and assist agencies in implementing the Act; and to alert the President and Congress to proposed Federal information programs and data banks which deviate from the standards and requirements of the Act; and

Judicial remedies allow the enforcement of the act through the courts by individuals and organizations in civil actions challenging denial of access to personal information or through suits by the Attorney General or any aggrieved person to enjoin violations or threatened violations of the Act.

Fifth, the bill requires the Commission to make a study of the major data banks and computerized information systems of other governmental agencies and of private organizations and to recommend any needed changes in the law governing their practices or the application of all or part of this legislation in order to protect the privacy of the individual.

Background

The Committee on Government Operations' ad hoc Subcommittee on Privacy and Information Systems conducted hearings on June 18, 19, and 20, 1974, to consider S. 3418, cosponsored by Senators Ervin, Percy, Muskie, and Ribicoff. The hearings were held jointly with the

Judiciary Committee's Subcommittee on Constitutional Rights which was considering the following legislation on related issues:

S. 2810, introduced by Senator Goldwater, to protect the constitutional right of privacy of individuals concerning whom identifying numbers or identifiable information is recorded by enacting principles of information practice in furtherance of amendments I, III, IV, X, and XIV of the U.S. Constitution;

S. 2542, introduced by Senator Bayh to protect the constitutional right of privacy of those individuals concerning whom records are maintained; and

S. 3116, introduced by Senator Hatfield, to protect the individual's right to privacy by prohibiting the sale or distribution of certain information.

COMMITTEE OVERSIGHT

These hearings continued the oversight by the Government Operations Committee of the development and proper management of automated data processing in the Federal Government and its concern for the effect on Federal-State relations of national and intergovernmental data systems involving electronic and manual transmission, sharing, and distribution of personal information about citizens.

Senator Ervin announced the joint hearings as Chairman of both subcommittees, in a Senate speech on June 11 in which he summarized the issues and described some of the complaints from citizens which have been received by Members of Congress, as follows:

> It is a rare person who has escaped the quest of modern government for information. Complaints which have come to the Constitutional Rights Subcommittee and to Congress over the course of several administrations show that this is a bipartisan issue which effects people in all walks of life. The complaints have shown that despite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information-gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy make it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.
>
> The complaints show that many Americans are more concerned than ever before about what might be in their records because Government has abused, and may abuse, its power to investigate and store information.
>
> They are concerned about the transfer of information from data bank to data bank and black list to black list because they have seen instances of it.
>
> They are concerned about intrusive statistical questionnaires backed by the sanctions of criminal law or the threat of it because they have been subject to these practices over a number of years.

S. 3418 provides an "Information Bill of Rights" for citizens and a "Code of Fair Information Practices" for departments and agencies of the executive branch.

Testimony and statements were received from Members of Congress who have sponsored legislation and conducted investigations into complaints from citizens; from Federal, State, and local officials including representatives of the Administration and certain departments and agencies, the Domestic Council Committee on Right to Privacy, the Commerce Department, Bureau of the Census, National Bureau of Standards, the General Services Administration, the Office of Telecommunications Policy; the National Governors Conference, the National Legislative Conference, the National Association for State Information Systems, and the Government Management Information Sciences. Many interested organizations and individuals with expert knowledge of the subject advised the Committee. These included the former Secretary of Health, Education, and Welfare, Elliot Richardson, authors of major studies, experts in computer technology, constitutional law, and public administration, the American Civil Liberties Union, Liberty Lobby, the National Committee for Citizens in Education, the American Society of Newspaper Editors, and others.

The provisions of the bill as reported, reflect the bill as introduced, with revisions based on testimony of witnesses at hearings, consultations with experts in privacy, computer technology, and law, representatives of Federal agencies and of many private organizations and businesses, as well as the staffs of a number of congressional committees engaged in investigations related to privacy and governmental information systems.

The Committee finds that the need for enactment of these provisions is supported by the investigations and recommendations of numerous congressional committees, reports of bar associations, and others organizations, and conclusions of governmental study commissions.

To cite only a few, there are:

Earlier studies of computers and information technology by the Senate Committee on Government Operations and the current hearings and studies relating to S. 3418;

The hearings and studies on computers, data banks and the bill of rights and other investigations of privacy violations before the Constitutional Rights Subcommittee;

The hearings and studies of computer privacy and government information-gathering before the Judiciary Administrative Practices Subcommittee;

The hearings on insurance industries and other data banks before the Judiciary Antitrust Subcommittee;

The hearings on abuses in the credit reporting industries and on protection of bank records before the Senate Banking, Housing and Urban Affairs Committee;

Investigations over many years by the House Government Operations Committee; and

Finally, there are many revelations during the hearings before the Select Committee on Watergate of improper access, transfer and disclosure of personal files and of unconstitutional, illegal or improper investigation of and collection of personal information on individuals.

Particularly supportive of the principles and purposes of S. 3418 are the following reports sponsored by Government agencies:

1. "Legal Aspects of Computerized Information Systems" by the Committee on Scientific and Technical Information, Federal Council of Science and Technology, 1972.

2. "Records, Computers and the Rights of Citizens", Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Department of Health, Education and Welfare, July 1973.

3. "Databanks in a Free Society, Computers, Record-Keeping and Privacy", of the Computer Science and Engineering Board, National Academy of Sciences, by Alan F. Westin and Michael Baker.

4. Technical Reports by Project Search Law Enforcement Assistance Administration, Department of Justice.

5. A draft study by the Administrative Conference of the United States on Interagency Transfers of Information.

6. Report by the National Governors Conference.

7. Reports by international study bodies.

The ad hoc subcommittee has initiated two surveys of the Governors and of the attorneys general of the States which are producing responses supportive of congressional legislation on privacy and Federal computers and information technology. They also reveal strong efforts in State and local governments to enact similar or stronger legislation to protect privacy.

The need for the bill is also evident from the sample of legal literature and public administration articles and press articles reprinted in the appendix of the subcommittee hearings.

Finally, there are the complaints of information abuses received by many Members of Congress and diligently investigated by each of them.

Dr. Alan F. Westin, director of the 1972 National Academy of Sciences Project, reported that the study suggested "six major areas of priority for public action: laws to give individuals a right of notice, access, and challenge to virtually every file held by local, State, and national government, and most private record systems as well; promulgation of clearer rules for data-sharing and data-restriction than we now have in most important personal data files; rules to limit the collection of unnecessary and overbroad personal data by any organization; increased work by the computer industry and professionals on security measures to make it possible for organizations to keep their promises of confidentiality; limitations on the current, unregulated use of the Social Security number; and the development of independent, 'information-trust' agencies to hold especially sensitive personal data, rather than allowing these data to be held automatically by existing agencies."

Witnesses cited the failure of legislation and judicial decisions to keep pace with the growing efficiency of data usage by promulgating clear standards for data collection, data exchange, and individual access rights. Similarly, many other witnesses before Congress agreed

with his judgment that the mid-1970's is precisely the moment when such standards need to be defined and installed if the managers of large data systems, and the specialists of the computer industry, are to have the necessary policy guidelines around which to engineer the new data systems that are being designed and implemented.

Dr. Westin cautioned:

> To delay congressional action in 1974–75, therefore, is to assure that a large number of major data systems will be built, and other existing computerized systems expanded, in ways that will make it extremely costly to alter the software, change the file structures, or reorganize the data flows to respond to national standards. And beyond the money, such late changes threaten to jeopardize many operations in vital public services that will be increasingly based on computerized systems—national health insurance, family assistance plans, national criminal-offender records, and many others. In fact, these systems may become so large, so expensive, and so vital to so many Americans that public opinion will be put to a terrible choice—serious interruption of services *or* installation of citizen-rights measures.

The spread of the data bank concept, the increasing computerization of sensitive subject areas relating to people's personal lives and activities, and the tendency of government to put information technology to uses detrimental to individual privacy were detailed by Professor Arthur Miller. He stated:

> Americans today are scrutinized, measured, watched, counted, and interrogated by more governmental agencies, law enforcement officials, social scientists and poll takers than at any other time in our history. Probably in no Nation on earth is as much individualized information collected, recorded and disseminated as in the United States.
>
> The information gathering and surveillance activities of the Federal Government have expanded to such an extent that they are becoming a threat to several of every American's basic rights, the rights of privacy, speech, assembly, association, and petition of the Government.
>
> * * * * * * *
>
> I think if one reads Orwell and Huxley carefully, one realizes that "1984" is a state of mind. In the past, dictatorships always have come with hobnailed boots and tanks and machineguns, but a dictatorship of dossiers, a dictatorship of data banks can be just as repressive, just as chilling and just as debilitating on our constitutional protections. I think it is this fear that presents the greatest challenge to Congress right now.

Professor Miller characterized the reported bill as "a major step in developing a rationale regulatory scheme for achieving an effective balance between a citizen and the Government in the important field of information privacy. The creation of a Privacy Protection Commission with broad power of investigation, reporting, and suasion seems to me to be an effective way of developing policy in this rapidly

changing environment. Also worthy of enthusiastic support is Title II of the proposed legislation. We simply cannot allow more time to pass without developing standards of care with regard to the gathering and handling of personal information. In that regard, S. 3418 goes a long way to establish the much needed information bill of rights."

The four-year survey by the Constitutional Rights Subcommittee, intended as an aid to Congress in evaluating pending legislation, demonstrates the need for requiring the following Congressional action:

> Explicit statutory authority for the creation of each data bank, as well as prior examination and legislative approval of all decisions to computerize files;
>
> Privacy safeguards built into the increasingly computerized government files as they are developed, rather than merely attempting to supplement existing systems with privacy protections;
>
> Notification of subjects that personal information about them is stored in a Federal data bank and provision of realistic opportunities for individual subjects to review and correct their own records;
>
> Constraints on interagency exchange of personal data about individuals and the creation of interagency data bank cooperatives;
>
> The implementation of strict security precautions to protect the data banks and the information they contain from unauthorized or illegal access; and
>
> Continued legislative control over the purposes, contents and uses of government data systems.

HEW Report

Another report reflecting major provisions of S. 3418 is that rendered by the Secretary's Advisory Committee on Automated Personal Data Systems to the Department of Health, Education and Welfare. Former Secretary Elliot Richardson described their findings in his testimony.

The report found that "concern about computer-based record keeping usually centers on its implications for personal privacy, and understandably so if privacy is considered to entail control by an individual over the uses made of information about him. In many circumstances in modern life, an individual must either surrender some of that control or forego the services that an organization provides. Although there is nothing inherently unfair in trading some measure of privacy for a benefit, both parties to the exchange should participate in setting the terms."

"Under current law, a person's privacy is poorly protected against arbitrary or abusive record-keeping practices." For this reason, as well as because of the need to establish standards of record-keeping practice appropriate to the computer age, the report recommends the enactment of a Federal "Code of Fair Information Practice" for all automated personal data systems. The Code rests on five basic prin-

ciples that would be given legal effect as "safeguard requirements" for automated personal data systems.

> There must be no personal data record-keeping systems whose very existence is secret.
>
> There must be a way for an individual to find out what information about him is in a record and how it is used.
>
> There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
>
> There must be a way for an individual to correct or amend a record of identifiable information about him.
>
> Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.*

The Advisory Committee recommended "the enactment of legislation establishing a Code of Fair Information Practice for all automated personal data systems as follows:

> The Code should define "fair information practice" as adherence to specified safeguard requirements.
>
> The Code should prohibit violation of any safeguard requirement as an "unfair information practice."
>
> The Code should provide that an unfair information practice be subject to both civil and criminal penalties.
>
> The Code should provide for injunctions to prevent violation of any safeguard requirement.
>
> The Code should give individuals the right to bring suits for unfair information practices to recover actual, liquidated, and punitive damages, in individual or class actions. It should also provide for recovery of reasonable attorneys' fees and other costs of litigation incurred by individuals who bring successful suits."

Pending the enactment of a code of fair information practice, the Advisory Committee also recommended that all Federal agencies apply these requirements to all Federal systems, and assure through formal rulemaking that they are applied to all other systems within reach of the Federal government's authority. Beyond the Federal Government, they urged that state and local governments, the institutions within reach of their authority, and all private organizations adopt the safeguard requirements by whatever means are appropriate.

Revolutionary changes in data collection, storage and sharing were described by Senator Goldwater, who was one of many witnesses who called for enactment of the recommendations of the HEW Advisory Committee. He stated:

> Computer storage devices now exist which make it entirely practicable to record thousands of millions of characters of information, and to have the whole of this always available

Records, Computers, and the Rights of Citizens, U.S. Department of Health, Education and Welfare, 1973, p. xx.

> for instant retrieval . . . Distance is no obstacle. Communications circuits, telephone lines, radio waves, even laster beams, can be used to carry information in bulk at speeds which can match the computer's own. Time-sharing is normal . . . we are now hearing of a system whereby it is feasible for there to be several thousands of simultaneous users or terminals. Details of our health, our education, our employment, our taxes, our telephone calls, our insurance, our banking and financial transactions, pension contributions, our books borrowed, our airline and hotel reservations, our professional societies, our family relationships, all are being handled by computers right now. Unless these computers, both governmental and private, are specifically programmed to erase unwanted history, these details from our past can at any time be reassembled to confront us . . . We must program the programmers while there is still some personal liberty left.

The Committee has found that the concern for privacy is a bipartisan issue and knows no political boundaries. President Ford, as Vice-President, chaired a Domestic Council Committee on the Right of Privacy which was established by President Nixon in February 1974. In recent address on the subject, he stated:

> In dealing with troublesome privacy problems, let us not, however, scapegoat the computer itself as a Frankenstein's monster. But let us be aware of the implications posed to freedom and privacy emerging from the ways we use computers to collect and disseminate personal information. A concerned involvement by all who use computers is the only way to produce standards and policies that will do the job. It is up to us to assure that information is not fed into the computer unless it is relevant.
>
> Even if it is relevant, there is still a need for discretion. A determination must be made if the social harm done from some data outweighs its usefullness. The decision-making process is activated by demands of people on the government and business for instant credit and instant services. Computer technology has made privacy an issue of urgent national significance. It is not the technology that concerns me but its abuse. I am also confident that technology capable of designing such intricate systems can also design measures to assure security.

FEDNET

In the same address, the Vice-President called attention to FEDNET and problems involved in a proposed centralization of computer facilities which concerned several Congressional committees and which provisions in S. 3418 would correct. He stated:

> The Government's General Services Administration has distributed specifications for bids on centers throughout the country for a massive new computer network. It would have the potential to store comprehensive data on individuals and institutions. The contemplated system, known as FEDNET, would link Federal agencies in a network that would allow

> GSA to obtain personal information from the files of many Federal departments. It is portrayed as the largest single governmental purchase of civilian data communication in history.
>
> I am concerned that Federal protection of individual privacy is not yet developed to the degree necessary to prevent FEDNET from being used to probe into the lives of individuals. Before building a nuclear reactor, we design the safeguards for its use. We also require environmental impact statements specifying the anticipated effect of the reactor's operation on the environment. Prior to approving a vast computer network affecting personal lives, we need a comparable privacy impact statement. We must also consider the fallout hazards of FEDNET to traditional freedoms.

Examples

The revelations before the Select Committee to Investigate Presidential Campaign Activities concerning policies and practices of promoting the illegal gathering, use or disclosure of information on Americans who disagreed with governmental policies were cited by almost all witnesses as additional reasons for immediate congressional action on S. 3418 and other privacy legislation. The representative of the American Civil Liberties Union stated:

> Watergate has thus been the symbolic catalyst of a tremendous upsurge of interest in securing the right of privacy: wiretapping and bugging political opponents, breaking and entering, enemies lists, the Huston plan, national security justifications for wiretapping and burglary, misuse of information compiled by government agencies for political purposes, access to hotel, telephone and bank records; all of these show what government can do if its actions are shrouded in secrecy and its vast information resources are applied and manipulated in a punitive, selective, or political fashion.

Despite such current concern, Congressional studies and complaints to Congress show that the threats to individual privacy from the curiosity of administrators and salacious inquiries of investigators predated "Watergate" by many years. These have been described at length in the hearing record on S. 3418.

For example, under pain of civil and criminal sanctions, many people have been selected and told to respond to questions on statistical census questionnaires such as the following:

> How much rent do you pay?
>
> Do you live in a one-family house?
>
> If a woman, how many babies have you had? Not counting still births.
>
> How much did you earn in 1967?
>
> If married more than once, how did your first marriage end?
>
> Do you have a clothes dryer?
>
> Do you have a telephone, if so, what is the number?

Do you have a home food freezer?

Do you own a second home?

Does your TV set have UHF?

Do you have a flush toilet?

Do you have a bathtub or shower?

The studies show that thousands of questionnaires are sent out yearly asking personal questions, but people are not told their responses are voluntary; many think criminal penalties attach to them; it is difficult for them to find out what legal penalties attach to a denial of the information or what will be done with it. If they do not respond, reports show that they are subjected to telephone calls, certified follow-up letters, and personal visits. Much of this work is done by the Census Bureau under contract, and many people believe that whatever agency receives the responses, their answers are subject to the same mandatory provisions and confidentiality rules as the decennial census replies. A Senate survey revealed that in 3 years alone the Census Bureau had provided their computer services at the request of 24 other agencies and departments for conducting voluntary surveys covering over 6 million people. Other independent voluntary surveys were conducted by the agencies themselves on subjects ranging from bomb shelters, to smoking habits, to birth control methods, to whether people who had died had slept with the window open. The form usually asked for social security number, address and phone number.

One such survey technique came to light through complaints to Congress from elderly, disabled or retired people in all walks of life who were pressured to answer a 15-page form sent out by the Census Bureau for the Department of Health, Education and Welfare which asked:

What have you been doing in the last 4 weeks to find work?

Taking things all together, would you say you are very happy, pretty happy, or not too happy these days?

Do you have any artificial dentures?

Do you—or your spouse—see or telephone your parents as often as once a week?

What is the total number of gifts that you give to individuals per year?

How many different newspapers do you receive and buy regularly?

About how often do you go to a barber shop or beauty salon?

What were you doing most of last week?

Applicants for Federal jobs in some agencies, and employees in certain cases, have been subjected to programs requiring them to answer forms of psychological tests which contained questions such as these:*

*Senate Report 93-724, to accompany S. 1688. "To Protect the Privacy and Rights of Federal Employees." The report describes other similar programs for soliciting, collecting or using personal information from and about applicants and employees. S. 1688 has been approved by the Senate five times.

I am very seldom troubled by constipation.

My sex life is satisfactory.

At times I feel like swearing.

I have never been in trouble because of my sex behavior.

I do not always tell the truth.

I have no difficulty in starting or holding my bowel movements.

I am very strongly attracted by members of my own sex.

I like poetry.

I go to church almost every week.

I believe in the second coming of Christ.

I believe in a life hereafter.

My mother was a good woman.

I believe my sins are unpardonable.

I have used alcohol excessively.

I loved my Mother.

I believe there is a God.

Many of my dreams are about sex matters.

At periods my mind seems to work more slowly than usual.

I am considered a liberal "dreamer" of new ways rather than a practical follower of well-tried ways. (a) true, (b) uncertain, (c) false.

When telling a person a deliberate lie, I have to look away, being ashamed to look him in the eye. (a) true, (b) uncertain, (c) false.

First Amendment Programs: the Army

Section 201(b)(7) prohibits departments and agencies from undertaking programs for gathering information on how people exercise their First Amendment rights. Section 201(a) prevents them from collecting and maintaining information which is not relevant to a statutory purpose.

The need for these provisions have been made evident in many ways. In addition to federal programs for asking people questions such as whether they "believe in the second coming of Christ," there have been numerous other programs affecting First Amendment rights.

One of the most pervasive of the intrusive information programs which have concerned the Congress and the public in recent years involved the Army surveillance of civilians, through its own records and those of other federal agencies. The details of these practices have been documented in Congressional hearings and reports and were summarized by Senator Ervin as follows:*

Hearings before the Subcommittee on Constitutional Rights of the Judiciary Committee, 4 *Columbia Human Rights Review* (1972) Hearings, 92d Cong., 2d sess. February 1971.

Despite First Amendment rights of Americans, and despite the constitutional division of power between the federal and state governments, despite laws and decisions defining the legal role and duties of the Army, the Army was given the power to create an information system of data banks and computer programs which threatened to erode these restrictions on governmental power.

Allegedly for the purpose of predicting and preventing civil disturbances which might develop beyond the control of state and local officials, Army agents were sent throughout the country to keep surveillance over the way the civilian population expressed their sentiments about government policies. In churches, on campuses, in classrooms, in public meetings, they took notes, taperecorded, and photographed people who dissented in thought, word or deed. This included clergymen, editors, public officials, and anyone who sympathized with the dissenters.

With very few, if any, directives to guide their activities, they monitored the membership and policies of peaceful organizations who were concerned with the war in Southeast Asia, the draft, racial and labor problems, and community welfare. Out of this surveillance the Army created blacklists of organizations and personalities which were circulated to many federal, state and local agencies, who were all requested to supplement the data provided. Not only descriptions of the contents of speeches and political comments were included, but irrelevant entries about personal finances, such as the fact that a militant leader's credit card was withdrawn. In some cases, a psychiatric diagnosis taken from Army or other medical records was included.

This information on individuals was programmed into at least four computers according to their political beliefs, or their memberships, or their geographic residence.

The Army did not just collect and share this information. Analysts were assigned the task of evaluating and labeling these people on the basis of reports on their attitudes, remarks and activities. They were then coded for entry into computers or microfilm data banks.

General Statement

The premise underlying this legislation is that good government and efficient management require that basic principles of privacy, confidentiality and due process must apply to all personal information programs and practices of the Federal Government, and should apply to those of State and local government as well as to those of the organizations, agencies and institutions of the private sector.

The need for such a general legislative formula is made necessary by the haphazard patterns of information swapping among government agencies, the diversity of confidentiality rules and the unevenness of their application within and among agencies. The lack of self-restraint in information-gathering from and about citizens on the part of some agencies has demonstrated the potential throughout government for

imposing coercive information burdens on citizens or for invading areas of thought, belief or personal life which should be beyond the reach of the Federal data collector.

* * *

The myriad rules and regulations reflecting many years of ad hoc policy decisions to meet the information needs of administrators facing problems of the political moment will, under this bill, be replaced by a rule of law. The Committee emphasizes that enactment of such general legislation in no way precludes specific legislation to govern records for special programs in such areas as tax, finance, health, welfare, census, and law enforcement. Furthermore, it should not be construed as a final statement by Congress on the right of privacy and other related rights as they may be developed or interpreted by the courts.

* * *

The Committee affirms that the present statutory division of executive branch power among the departments and agencies and bureaus promotes accountability and is most conducive to legislative oversight, Presidential management, and responsiveness to the public will. We believe that the creation of formal or de facto national data banks, or of centralized Federal information systems without certain statutory guarantees would tend to defeat these purposes, and threaten the observance of the values of privacy and confidentiality in the administrative process. The Committee therefore intends in S. 3418 to require strict reporting by agencies and departments and meaningful congressional and executive branch review of any proposed use of information technology which might tend to further such negative developments.

* * *

The Committee recognizes that the computer is an instrument which is absolutely essential to the proper transaction of many government programs, and that the collection of information from the individual is absolutely necessary to carry out those programs.

Also necessary to modern government is the science of management of the many aspects of information technology and its related professional personnel which have been incorporated very rapidly into the administrative processes of the Federal Government.

At the same time, however, the Committee believes that in the management of computer systems and all other aspects of information technology, a special status must be accorded to the issue of individual privacy, that is, the right of an individual to have such gathering of personal information as may be collected by the Government confined to that for which there is a legitimate use, and then secondly, after it is gathered, to have access to that information confined to those who have a governmental end in view for its use, and thirdly, to be assured by government that there is as little leakage as possible to unauthorized persons.

The present legislation is designed to foster these goals in the administrative processes of the executive branch. The Committee believes that the bill strikes a balance between governmental needs and the personal freedoms of the individual.

The complexities and scale of modern government make it impossible for Congress or the courts to monitor every decision made which involves personal information. The bill therefore depends partly for its enforcement on the individual data subject and makes that person a participant in government's decision to exercise its information power over an individual.

* * *

The Committee is convinced that legislation cannot and should not be neutral toward the information technology by means of which the Federal Government affects individual rights. Certain kinds of information should not be collected or maintained or disclosed by government agencies because to do so is either unconstitutional, unfair, unwise, or simply bad management of the people's business. This means, furthermore, that certain computer hardware and software used to operate the information systems of government should provide features which will promote the necessary security of any part of the system and the confidentiality of the information processed and handled by means of it.

* * *

The bill does not rest solely on the findings of any one report or study, but on review and consideration of all of the studies cited here.

The Committee is convinced that effective legislation must provide standards for and limitations on the information power of government. Providing a right of access and challenge to records, while important, is not sufficient legislative solution to threats to privacy. Contrary to the views of Administration spokesmen it is not enough to tell agencies to gather and keep only data which is reliable by their rights for whatever they determine is their intended use, and then to pit the individual against government, armed only with a power to inspect his file, and a right to challenge it in court if he has the resources and the will to do so.

To leave the situation there is to shirk the duty of Congress to protect freedom from the incursions by the arbitrary exercise of the power of government and to provide for the fair and responsible use of that power. For this reason, the Committee deems especially vital the restrictions in section 201 which deal with what data are collected and by what means. For this reason, the establishment of the Privacy Commission is essential as an aid to enforcement and oversight.

The Committee views the standards of statutory relevance for data gathering as minimum and as paving the way for more specific guarantees in each area. The Committee rejects in part and supplements the position of the White House representative, the Chairman of the Domestic Council Committee on Right of Privacy, who testified that "the Federal Government should collect from individuals only the amount and types of information that are reasonably necessary for public protection." He stated "I do not think it is possible to develop a standard of reasonableness in any more precise way than to ask people to exercise their very best judgment and to exercise the utmost restraint in the amount of information they collect."

The Committee found many helpful definitions of privacy and confidentiality in seeking to define the concepts and principles developed in the provisions of S. 3418.

A useful statement is offered by the report on Data Banks in a Free Society project by the National Academy of Sciences, which distinguishes them in the following terms:

> *Privacy* is independent of technological safeguards; it involves the social policy issues of what information should be collected at all and how much information should be assembled in any one information system. (For purposes of the principles implemented by this bill for the Federal executive branch, the Committee means this to include constitutional and statutory prohibitions or restraints.)
>
> *Confidentiality* is the central issue for which technological safeguards are relevant. Where an organization has promised those from whom it collects information that unauthorized uses will not be made by persons inside or outside that agency, making good that promise of confidentiality requires record security controls in both manual and computerized files.

* * *

"Privacy", then, is a shorthand term for the restraint on the power of government to investigate individuals, to collect information about their personal lives and activities in society or in ways which are banned by the Constitution, or for reasons which have little or nothing to do with the purpose of government or of the agency involved, as their powers are defined by the Constitution and specific statutes.

Therefore, the Committee believes that the conclusions of study groups set up in the executive branch to study computer technology must be supplemented by the complaints from citizens and evidence gathered by numerous congressional committees on the over-reach of its information power by the Federal executive branch. This characteristic distinguishes S. 3418 from other proposals on "privacy."

State Laws

S. 3418 is further needed to complement State and minicipal laws and regulations which have been adopted to protect individual privacy and confidentiality of records, and which, in some cases, provide more detailed and more effective protections than S. 3418. Governors and others have expressed concern that despite all the States may do to provide guarantees, they are not effective once the data are integrated in a Federal information system or transferred to a Federal data bank. S. 3418 will safeguard and supplement the efforts of State legislatures.

Coverage: Private, State and Local

As reported, the bill applies to Federal personal information systems, whether automated or manual, and to those of State, local and private organizations which are specifically created or substantially altered through grant, contract or agreement with Federal agencies, where the agency causes provisions of the act to be applied to such systems or files or relevant portions.

As introduced, S. 3418 applied to all governmental and private organizations which maintained a personal information system, under supervision of a strong regulatory body, with provision for delegating power to State instrumentalities.

The Committee has cut back on the bill's original coverage and ordered the Privacy Commission to make a study of State, local and private data banks and recommend precise application of the Act where needed.

The original coverage reflected the recommendations of the HEW Secretary's Committee for "enactment of its code of fair information practice for all automated personal data systems," but which noted that it would "wisely be applied to all personal data systems whether automated or manual."

Hearing witnesses and other commentators advocated nationwide application of the Act to protect individual privacy and other rights from invasion by Government and the institutions and organizations of society.

Total coverage was advocated by the representative of the American Civil Liberties Union citing examples of cases and programs to show that information collected by State, local and private institutions can be every bit as harmful to the individual. These included the reported need for additional controls over the retail credit industry, whose five largest companies maintain files on 54 million people; the Medical Information Bureau in Greenwich, Connecticut, a major source of medical information on 13 million Americans for life insurance companies; the use by the banking industry of an Electronic Funds Transfer System to centralize an individual's charges all over the community and automatically deduct them from the individual's bank account; the uncontrolled access to customer records and cancelled checks afforded by financial institutions to law enforcement officials and other investigators in the absence of subpena and notice to the individual.

Professor Miller testified in 1971 on behalf of a regulatory commission with power to embrace the activities of "non-Federal information gatherers that might adversely affect the rights we are trying to protect. The regulators should be particularly attentive to the interlocking relationships that have begun to spring up between Federal and local data handlers in the law enforcement field and the fact that many of the Nation's major corporations maintain dossiers on millions of Americans. Close scrutiny of the latter category of data banks is becoming imperative because there is growing reason to believe that these files are exchanged both within the private sector and with law enforcement and surveillance groups at all levels of government. In short, once standards are established for Federal systems I believe that it eventually will become necessary to apply them to certain non-Federal systems."

Similar findings of interlinking networks for the governmental and private sectors were found by the Academy of Sciences project.

Professor Vern Countryman, in an article submitted for the hearing record, has detailed cases, congressional hearings, and practices involving privately compiled dossiers by commercial compilers, punitive compilers, and benevolent compilers.

Reports filed for the hearing record from the Freedom of Information Center of the University of Missouri School of Journalism, describe investigative practices and intrusive data-gathering technique in the private sector.

Problems of privacy, standards, confidentiality and security in medical and health records programs were described for the subcommittee by doctors in private practice and in State government.

Extension of legislative coverage to student records procedures for gathering, disclosure, and dire process in educational records was advocated by Senator James L. Buckley and by witnesses for the Citizens Committee for Education.

Other witnesses advocated coverage of State and local systems, but not of the private sector.

Despite calls by these and other witnesses for total or partial coverage, the Committee was persuaded to delay a decision on total application by considerations of time and investigative resources for developing a full hearing record and for drafting the needed complex legislative solution for information abuses in the private sector, beyond those presently covered by the Fair Credit Reporting Act and its pending amendments.

Former Secretary of Health, Education, and Welfare Elliot Richardson noted the lack of a precise hearing record and suggested legislation "to establish authority in an existing Federal agency or in some new instrumentality established in part for that purpose, to make inquiry, hold hearings, and report to Congress if it finds a *prima facie* showing of need for legislation to assure fair information practice in some particular industry or other segment of the nongovernmental organizations of America. Congress could then take whatever action toward developing additional legislation seemed necessary."

Mr. Richardson endorsed coverage of State and local activities "substantially affected by their relationships with Federal agencies, as a consequence of (1) Federal fiscal contributions, (2) Federal record-keeping or data-collection and reporting requirements, or (3) cooperative arrangements among intergovernmental personal data system."

Dr. Westin, while endorsing coverage of intergovernmental computers systems, opposed the total coverage of the original bill, citing "the impracticality and dangers involved in trying to regulate and register many tens or hundreds of thousands of files of every kind." He recommended "an instrumentality to lead private organizations to adopt codes of fair information practice as thier voluntary policies, and proposed creating a national commission on private, interstate personal data systems." This commission should, testified Dr. Westin, "examine the conduct of those nationwide personal data systems that affect the rights, opportunities, and benefits of Americans, holding hearings as necessary and with a strong, competent staff to make on-site visits and study the real practices of organizations, not just their formal policies.

"The creation of such a commission should provide an extremely valuable force acting on the private sector. It would push privacy, confidentiality, and due process issues to the top of the organizational agenda, and into the design, testing, and operational thinking of data-system managers and their staffs. It would move the computer industry and computer professionals into high gear, as consultants to the user organizations, developers of new techniques and materials, and innovators in cost-effective responses."

Numerous representatives of private organizations and of business and industry opposed the total coverage of the bill, citing the lack of hearing record, the existing requirements of the Fair Credit Reporting Act, and prohibitive costs of implementing S. 3418 in the private sector without passing on the costs in consumer services. Most indicated support for or lack of opposition to, a commission study of privacy invasions by the private sector.

RIGHT OF ACCESS AND CHALLENGE

The Committee believes that the size of the Federal Government, the sheer number of personal records it must handle, and the growing complexities of information technology require that the full protections against abuses of the power of government to affect the privacy of the individual and the confidentiality of personal information must depend in part upon the participation of the individual in monitoring the maintenance and disclosure of his own file.

To this end, we agree with the members of numerous respected study bodies that an individual should have the right to discover if he is the subject of a government file, to be granted access to it, to be able to assure the accuracy of it, and to determine whether the file has been abused by improper disclosure.

The Committee agrees with the conclusion of one government study that "In the majority of cases, the citizen's right of access to information kept on him by the Federal Government will not interfere with the ongoing program of the agency. In addition, giving the individual a right of access often will be a desirable adjunct to any other system designed to insure file accuracy."

Furthermore, the Committee adopts the timely observation of one scholar from the Council on Science of Technology study that "giving the individual maximum ability to examine what the Government knows on the person should help promote citizen confidence in activities of the Federal Government and is essential to assure that notions of due process are employed when decisions are made on the basis of personal information."

So important does the Committee consider procedures required by the bill on this matter that it is determined that any exemptions from such provisions sought under the rule-making scheme of the bill must be kept to an absolute minimum and must not be made on the basis of parochial agency concerns. It finds support for this stand in the conclusion of the report of the HEW Secretary's Advisory Committee on Automated Personal Data Systems that:

> No exemption from or qualification of the right of data subjects to have full access to their records should be granted unless there is a clearly paramount and strongly justified societal interest in such exemption or qualification. . . . The instances in which it can be convincingly demonstrated that there is a paramount society interest in depriving an individual of access to data about himself would seem to be rare. (pp. 61, Report.)

The exemptions allowed from observance of these standards are for three purposes only, national defense and foreign policy and

certain law enforcement investigative and intelligence matters where access and challenge rights are found to damage the purpose for which the information was collected.

The Committee recognizes that while many agencies afford such rights, many agencies deny them with respect to certain files. Allowing only these narrow areas for exemption may well promote the reassessment of existing practices whereby individuals are deprived of full access to records about themselves, and some agencies, in the year before the Act takes effect, may well see fit to seek special legislation permitting special treatment of certain files they hold. Meanwhile, the Committee is persuaded by the language of the HEW report:

> Many organizations are likely to argue that it is not in the interest of their data subjects to have full access. Others may oppose full access on the grounds that it would disclose the content of confidential third-party recommendations or reveal the identity of their sources. Still others may argue that full access should not be provided because the records are the property of the organization maintaining the data system. Such objections, however, are inconsistent with the principle of mutuality necessary for fair information practice.

The relevance of the rights of access and challenge to the principle of accountability in government, to efficient achievement of management goals and to a public sense of social justice is recognized in a 1970 report made by the Project SEARCH group to the Justice Department. That report called for a citizen's right to access and challenge to certain law enforcement records, but it stated the following reasons for its conclusions which the committee finds worthy of general application:

> First, an important cause of fear and distrust of computerized data systems has been the feelings of powerlessness they provoke in many citizens. The computer has come to symbolize the unresponsiveness and insensitivity of modern life. Whatever may be thought of these reactions, it is at least clear that genuine rights of access and challenge would do much to disarm this hostility.
>
> Second, such rights promise to be the most viable of all the possible methods to guarantee the accuracy of data systems. Unlike more complex internal mechanisms, they are triggered by the most powerful and consistent of motives, individual self-interest.
>
> Finally, it should now be plain that if any future system is to win public acceptance, it must offer persuasive evidence that it is quite seriously concerned with the rights and interests of those whose lives it will record. The committee can imagine no more effective evidence than authentic rights of access and challenge.[1]

[1] Project SEARCH, Committee on Security and Privacy, Technical Report No. 2, July 1970, p. 28.

Law Enforcement Files

Title II of S. 3418 sets general standards of fair records keeping which apply to practically all government files, including those maintained by law enforcement agencies. Although various committees of the Congress [1] have been considering legislation which specifically addresses confidentiality of law enforcement files, the Committee is of the view that prospects for that legislation is sufficiently unclear so that S. 3418 should apply in its general terms to such files until such time as the law enforcement privacy legislation is enacted.

Therefore the Committee decided that, to the extent feasible, S. 3418 should apply to law enforcement files but that such application should not be inconsistent with the two major criminal justice privacy bills, introduced early this year, S. 2963 by Senator Ervin and S. 2964 by Senator Hruska on behalf of the administration. S. 3418 as amended by the Committee would apply the general standards of title II, including the general updating and accuracy requirements and provisions affording right of access to most law enforcement files.

The Committee recognizes, however, that there are two general classes of files maintained by agencies with law enforcement functions, criminal history or record files on the one hand and intelligence and investigative files on the other. The first class of information, defined for the purposes of S. 3418 as "criminal history information" includes routine records of arrests and court dispositions sometimes called rap sheets. As a general principle these records are subject to all the requirements of title II including the right of access provision. This is entirely consistent with both the Ervin and administration criminal justice privacy legislation. Indeed, Director Kelly of the FBI, in testimony before the Subcommittee on Constitutional Rights, expressed support for the general access and challenge provisions contained in the two criminal justice privacy bills and replicated in S. 3418:

> These bills provide for an individual to obtain access to his own criminal offender record, and also provide procedures for him to challenge that record. I support these provisions. Currently, the FBI provides copies of offender record information . . .

As for the other general provisions of title II, none of these provisions are inconsistent with the criminal justice privacy legislation in particular as they apply to criminal history information. Furthermore, S. 3418 permits each agency to promulgate its own regulations implementing the Act and this should provide sufficient flexibility so that the Attorney General will not undermine good law enforcement practices in promulgating regulations. Indeed, since early this year the Justice Department has been drafting regulations which address most of the basic issues raised by S. 3418. Those regulations set certain standards for the operation of any routine exchange of criminal history information by the FBI and for the funding of criminal history record systems on the State and local level by the Law Enforcement Assistance Administration. Although the Justice Department might have to

[1] The Senate Subcommittee on Constitutional Rights and House Subcommittee on Civil Rights and Constitutional Rights.

carefully review these regulations, if this legislation is passed, their scope and thrust are essentially what would be required of the Department of Justice by this legislation.

The second class of information generally maintained by law enforcement agencies are intelligence, or investigative files. These files contain highly sensitive and usually confidential information collected by law enforcement officers in anticipation of criminal activity, such as by organized crime figures, or in the course of investigating criminal activity which has already occurred. It was the Committee's judgment, shared by most criminal justice privacy experts and reflected in the pending criminal justice privacy legislation, that all of the provisions of title II of S. 3418 could not be applied to such sensitive information. In particular, it would not be appropriate to allow individuals to see their own intelligence or investigative files. Therefore, the bill exempts such information from access and challenge requirements of title II. However, most of the other general accuracy and updating provisions would apply, subject, of course, to the rules and regulations issued by the agency head in the course of implementing such provisions.

Obviously, these general provisions on law enforcement records are not entirely adequate. The two criminal justice privacy bills address this subject in considerable detail and are the result of at least two years of careful study and revision by the Subcommittee on Constitutional Rights and the Justice Department. However, the Committee feels that general privacy legislation must assure subjects of law enforcement files at least these minimal rights until such time as the more comprehensive criminal justice legislation is passed.

Privacy Protection Commission

It is clear that many of the information abuses over the last decade could have been avoided with the help of an independent body of experts charged with protecting individual privacy as a value in government and society.

Commentators on privacy for years have also cited the need for such an agency to help deal in a systematic fashion with the great range of administrative and technological problems throughout the many agencies of the Federal Government.

Title I of S. 3418, as amended, establishes a Privacy Protection Commission composed of five experts in law, social science, computer technology, and civil liberties, business, and State and local government and supported by a professional staff. The Commission would be empowered to:

> Monitor and inspect Federal systems and data banks containing information about individuals;
>
> Compile and publish an annual U.S. Information Directory so that citizens and Members of Congress will have an accurate source of up-to-date information about the personal data-handling practices of Federal agencies and the rights, if any, of citizens to challenge their contents;
>
> Develop model guidelines for implementation of this act and assist agencies and industries in the voluntary development of fair information practices;

Investigate and hold hearings on violations of the Act, and recommend corrective action to the agencies, Congress, the President, the General Accounting Office, and the Office of Management and Budget;

Investigate and hold hearings on proposals by Federal agencies to create new personal information systems or modify existing systems for the purpose of assisting the agencies, Congress, and the President in their effort to assure that the values of privacy, confidentiality, and due process are adequately safeguarded; and

Make a study of the state of the law governing privacy-invading practices in private data banks and in State and local and multistate data systems.

Need for a Privacy Protection Unit

There is an urgent need for a permanent staff of experts within the Federal Government to inform Congress and the public of the data-handling practices of major governmental and private personal information systems. As a recent study by the Judiciary Subcommittee on Constitutional Rights graphically demonstrates, there has been a proliferation of Federal information systems and data banks which, if misused, can do irreparable harm to the privacy and economic well-being of millions of persons. "Data Banks and a Free Society," the study done for the National Academy of Sciences by Professors Alan F. Westin and Michael A. Baker, similarly demonstrates such harm inherent in large personal information systems maintained at all levels of government and by private industry.

Although recent attempts to turn Federal tax records into weapons of political and personal revenge have come to light, along with many other record abuses, the major threat to most Americans lies in the inadvertent, careless, and unthinking collection, distribution, and storage of records which may be inaccurate, incomplete, or irrelevant to legitimate governmental needs. This threat has grown tremendously as developments in telecommunications, photocopying, and computer technology have accelerated and with expanded data-swapping among government agencies and throughout private industry.

It is now clear that Congress, with its limited technical staff and multitude of functions, cannot keep track of these developments in every Federal agency and for every data bank with the depth of detail required for consistently constructive policy analysis. The Constitutional Rights Subcommittee data bank study and other agency-by-agency studies have each taken years to complete, and have documented the frustrations of agency delays, withholding of data, and camouflage of governmental activities. Citizens also have no place to turn to find out which agencies or companies maintain, distribute, and use personal information about them. Agencies and businesses would similarly benefit from the existence of an authoritative source of information about their record-keeping practices which would protect them from misinformed and inflamatory criticism.

In addition, there is an urgent need for a staff of experts somewhere in government which is sensitive both to the privacy interests of citizens and the informational needs of government and which can furnish expert assistance to both the legislative and executive branches.

In recent years, controversies over privacy and government data banks have arisen after executive branch decisions have been made. The Commission will serve the important purposes of raising and resolving privacy questions before government plans are put in operation. Agencies need help to incorporate newly-refined concepts of individual liberty into their current procedures without unnecessary disruption and confusion. Congress and the President need help in identifying those areas in which privacy safeguards are most urgently needed and in drafting legislation specifically tailored to those problem areas.

There are now over 100 privacy bills before Congress. Most are of unquestionable merit, but only a few can receive the kind of sustained attention to survive the legislative gauntlet. The proposed Commission would help Congress deal with those bills in two ways. First, it would obviate the necessity of enacting many of them into law by inducing agencies and industries to adopt their own fair information practices. Second, the Commission would help Congress and the President by narrowing down the range of legislative options and drafting bills designed to achieve a good "fit" between privacy values and other values in the context of often unique data-keeping activities.

It may well be that regulatory functions will eventually have to be added to the Commission's powers in order to assure that privacy, confidentiality, and due process become an integral part of governmental and private data systems. However, the Committee has decided not to address this area in the legislation pending the Commission's study.

The original version of S. 3418 would have created a Federal policy board with regulatory powers to investigate and issue cease and desist orders for violations of the Act. The Committee believes that it does not have sufficient evidence to support a case for vesting broad regulatory powers in a board charged with administrating the Act. Rather, a much more effective and less cumbersome procedure will permit an individual to seek enforcement of his rights under procedures established by each Federal agency. Ultimate enforcement of those rights and challenges to agency judgments would rest with United States District Courts. By taking this action, the Committee did not mean to preclude a future decision by the Congress to vest regulatory functions in the Commission to assure that privacy, confidentiality, and due process become an integral part of governmental and private data systems.

Public administration and privacy experts have urged a cautious approach to regulation on two grounds. First, there is much more that privacy advocates need to know about information systems before they are in a position to make demonstrably constructive regulatory policy proposals. Second, there is substantial evidence that agencies and companies are not inherently hostile to letting individuals have more of a say in what the files say about them, provided that the changes can be made in an orderly, efficient, and economically sound manner. The work of the Secretary of Health, Education, and Welfare's Advisory Committee on Automated Data Systems, Vice President Ford's Domestic Council Committee on the Right of Privacy, and the National Academy of Sciences Project on Computer Data Banks, clearly demonstrate that the right of privacy has its advocates within the executive branch. Testimony before the Committee by

State officials was nearly unanimous in citing a need for higher standards and better regulation of privacy practices in their jurisdictions. Statements by private industry representatives have persuaded the Committee that a substantial measure of industry cooperation can be anticipated.

Thus, the Committee believes that it would be a mistake for the Privacy Protection Commission to begin its work in an adversarial posture, either as a regulatory or ombudsman-type agency. Those roles may come in time, but they should be the product of specific legislation and come only after efforts to achieve voluntary reforms have failed. Meanwhile, awareness that the Commission might be vested by Congress with regulatory powers at some future time should have a salutory effect on those agencies which may be tempted to ignore its suggestions, or which fail to give its model guidelines the deference due them.

Locating the Privacy Unit

The Committee has concluded that the best place to vest these new functions would be in an independent commission. The decision was arrived at with some reluctance, because members of the Committee share the unwillingness of many Members of Congress to create still more independent commissions. On balance, however, the commission route seemed the best solution for the abuses and potential threats which have been documented.

Having concluded that an expert staff and an independent body was needed somewhere in the Federal Government to supply information and advice and conduct investigations, the Committee considered three alternatives, as described in testimony before Committee by Dr. Christopher H. Pyle. The first was to place the unit in the General Accounting Office, modeled on the Office of Federal Elections. The second was to locate it in the Office of Management and Budget, much like the Statistical Policy Division which polices Federal questionnaires. The third alternative was to create an independent commission.

The Committee chose not to recommend vesting the investigatory and advisory functions in the GAO because it would be unwise to dilute the GAO's important auditing function with this kind of substantive policy assignment. Except in rare instances, responsibility within Congress for policy development should rest with its committees. Also, placing the investigative role in the GAO might limit the unit's ability to study multi-state and commercial information systems not dependent upon the Federal budget, which is the focus of the GAO's attention.

Similar considerations persuaded the Committee that the unit could not achieve its full potential as part of the Office of Management and Budget. Moreover, the Committee was of the opinion that the privacy protection unit should be available to congressional committees as well as executive agencies—a relationship which could not be guaranteed by making it part of the President's staff. On the other hand, by creating the unit as a commission, its reports and expertise could be available to both the GAO and OMB.

The Committee received suggestions that creation of such an independent commission should be delayed in order to develop legislation charging it with the functions of dealing with classification and freedom of information issues, as well as privacy and civil liberties.

While they pose significant problems, these other two subject areas go to different considerations of government. Creation of a privacy commission is recognition of the fact that the Congress intends to afford access to the decision-making centers of government to interests which promote the privacy of individual Americans against overly-intrusive or arbitrary government information policies. To dilute the quality of that access, as institutionalized in the structure by the Privacy Commission, would defeat the purpose of the legislation. It would reduce the viability of privacy as a matter of concern in the Federal Government. By thus denying itself the full strength of the investigative help needed to protect privacy and due process in the years ahead, Congress would dilute, in turn, the quality of protections which it and the other branches of Government might otherwise afford to those amendments in the Bill of Rights which safeguard privacy.

The administration has opposed the creation of a commission partly for reasons of cost. It is the Committee's belief, however, that the Commission is vitally needed to promote the quality of legislative and administrative oversight which will provide a privacy bulwark for Americans in the years ahead. It is expected, furthermore, that the savings it will effect in the Federal Government will far outweigh the immediate cost.

Enforcement

The Act is enforceable in the courts with the aid of Congress and the Privacy Commission.

As Elliot Richardson, former Secretary of three executive branch Departments, informed the Committee:

> The requirements of fair information practice are so much in the interest of organizations, as well as of the individuals about whom records are maintained, that there should be little difficulty in agencies adhering to them and little occasion for court enforcement suits. Enforcement provisions are needed, however, to create a strong and reliable incentive to overcome the initial bureaucratic resistance to change that might otherwise prove to be a crucial obstacle to the prompt and full achievement of fair information practice. Frivolous suits, no doubt a matter of concern to some, would be promptly subject to motions for summary dismissal.

Except for the act of keeping secret data banks and improper disclosure by Commission employees, there are no criminal penalties in the Act. As introduced, the original bill contained strong criminal penalties for employees and others who violated or contributed to the violation of the Act. These penalties were deleted in Committee for two main reasons: the difficulties of effective enforcement through such criminal prosecutions and the possibility that the threat of prosecution may preclude that "Whistleblowing" and disclosure of wrongdoing to

Congress and the press which helps to promote "open government."

Instead, the mandates of S. 3418 are enforceable through the civil challenges of the Attorney General or of private citizens with real or suspected grievances or claims of violations of the Act. Given the difficulties of time and resources, private enforcement through litigation is not likely to affect more than glaring violations of the Act. Much will depend on the zeal and the good faith of the Attorney General and the President in enforcing the terms of the new law.

As always, the press and communications media will contribute to the enforcement of the Act through its investigation and exposure of wrongdoing, a function cased by the requirements in S. 3418 that decisions be made on the open record by responsible officials and that precise notices be published containing the details of government policy where it affects personal privacy.

Administratively, the agencies may be called to account by Congress and the President through the monitoring and investigative activities of the Privacy Commission and its reporting of violations.

Despite these guarantees, the Committee acknowledges there is no way that the Congress, the press, or the public can assure strict administrative observance of the exercise of the power of the Federal Government pursuant to the standards of the Act. There will no doubt be some diversity of views as to what constitutes compliance within particular agencies.

Realistically, therefore, the implementation of the Act rests, finally, with the departments and agencies of the executive branch and the good faith, ethical conduct and integrity of the Federal employees who serve in them.

SOCIAL SECURITY NUMBER AND IDENTIFIERS

As introduced, S. 3418 made it unlawful for any person to require an individual to disclose or furnish his Social Security account number for any purpose in connection with any business transaction or commercial or other activity, or to refuse to extend credit or make a loan or to enter into any other business transaction or commercial relationship with an individual because of refusal to disclose or furnish the number, unless the disclosure or furnishing of the number was specifically required by Federal law.

The Committee considers this usage of the number of a government file one of the most serious manifestations of privacy concerns in the Nation. However, it received conflicting evidence about the effects of this section, particularly the inordinate costs to the Federal Government and private businesses of changing to another identifier and reprogramming computers or reindexing files.

In view of the lack of ready independent data about the probable costs and effects of such a prohibition and in view of stricter limitations on transfer of and access to government files, the section was deleted in Committee by an 8 to 1 vote. At the same time, the issue was designated as a priority issue for study by the Privacy Commission and for report to Congress of specific legislative recommendations to meet the serious public concerns reflected in the original bill. In subsection 106(b)(1)(C), the Commission is required to examine and analyze "the use of license plate numbers, Social Security numbers,

universal identifiers, and other symbols to identify individuals in data banks and to access, integrate or centralize information systems and files."

The Committee realizes that the number is a major element in the national debate over privacy since a common numerical identifier or symbol to designate and index each person is an essential feature of a national data bank, or indeed, of any information system which allows creation of an instant dossier or which permits quick retrieval of all personal information which flows through that system about an individual.

In recent years the Social Security number has been the identifier most used in common by government agencies and private organizations to improve efficiency of services, aid management functions, prevent fraud and reduce errors in identification of people.

Citizens' complaints to Congress and the findings of several expert study groups have illustrated a common belief that a threat to individual privacy and confidentiality of information is posed by such practices. The concern goes both to the development of one common number to label a person throughout society and to the fact that the symbol most in demand is the Social Security number, the key to one government dossier. .

Of major concern is the possibility that the number may become a means of violating civil liberties by easing the way for intelligence and surveillance uses of the number for indexing or locating the person.

In this connection, a Constitutional Rights Subcommittee report on the intelligence-gathering by the military from its own agents and the files of other Government agencies, shows that individuals were often indexed in the Army computers by their Social Security numbers. Complaints to the Constitutional Rights Subcommittee also showed that government pressures people to disclose their Social Security number on administrative, statistical, and research questionnaires of all kinds, including income tax forms, HEW questionnaires asking whether elderly people buy newspapers and wear false teeth, and many others.

Every serviceman is now identified by his Social Security number, a development of intense concern to some groups who were not able to persuade congressional committees or the Pentagon to reverse the course.

A cross-section of such complaints appearing in the subcommittee hearings shows that people are pressured in the private sector to surrender their numbers in order to get telephones, to check out books in university libraries, to get checks cashed, to vote, to obtain drivers' licenses, to be considered for bank loans, and many other benefits, rights or privileges.

In many cases in the private sector, he is informed that the number is necessary for identification purposes, yet on its face, the Social Security card states that it is *not* to be used for identification purposes. This proviso was initially included in the Social Security program to prevent reliance on the card for identification because a person could acquire several of them under several identities and there frequently was no agency investigation of the information provided in order to obtain a number.

A list of the Federal Government's uses of the number, authorizations, and the texts of applicable statutes, Executive order, and regulations appears in the appendix of the hearings together with excerpts of Government reports on this subject.

The HEW Secretary's committee found that "the Federal Government itself has been in the forefront of expanding the use of the number, that its actions have actively promoted the tendency to depend more and more upon the number as an identifier—of workers, taxpayers, automobile drivers, students, welfare beneficiaries, civil servants, servicemen, veterans, pensioners, and so on." It concluded: "If use of the SSN as an identifier continues to expand, the incentives to link records and to broaden access to them are likely to increase. Until safeguards such as we have recommended . . . have been implemented, and demonstrated to be effective, there can be no assurance that the consequences for individuals of such linking and accessibility will be benign. At best, individuals may be frustrated and annoyed by unwarranted exchanges of information about them. At worst, they may be threatened with denial of status and benefits without due process, since at the present time record linking and access are, in the main, accomplished without any provision for the data subject to protest, interfere, correct, comment, and in most instances, even to know what linking of which records is taking place for what purposes."

While specific laws mandate or have been interpreted to permit the use of the number in a few Federal programs, most agencies have proceeded to use it by regulation or directive. Executive Order 9397 of 1943 found it "desirable in the interest of economy and orderly administration that the Federal Government move towards the use of a single unduplicated numerical identification system of accounts", and ordered that "any Federal department, establishment or agency shall, whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize exclusively the Social Security account numbers."

While some have cited this order as authority for the Federal usage, the HEW report found otherwise, noting, "It has been suggested that Executive Order 9397 was intended to apply only to instances when Federal agencies seek to number records, such as employment, attendance, performance, or medical records. . . . To interpret the order as applying to all kinds of Federal agency record systems is arguably beyond the meaning of its language. In any case, it appears that Federal agencies are free to use the SSN in any way they wish, and no instance has come to our attention in which the order has been invoked to compel or limit an agency's use of the SSN." (p. 117)

The HEW Secretary's committee came to the following conclusions about the need for legislation on this matter: "If the SSN is to be stopped from becoming a de facto Standard Universal Identifier, the individual must have the option not to disclose his number unless required to do so by the Federal Government for legitimate Federal program purposes, and there must be legal authority for his refusal. Since existing law offers no such clear authority, we recommend specific, preemptive, Federal legislation providing that the individual has the right to refuse to disclose his SSN to any person or organiza-

tion that does not have specific authority provided by Federal statute to request it . . . and the right to redress if his lawful refusal to disclose his SSN results in the denial of a benefit."

The report contained other recommendations about the need for constraints on the use of the number and on its dissemination, and it cited the need for congressional review of all present Federal requirements for use of the number to determine whether they should be continued, repealed, or modified.

The Committee expects the Privacy Commission study to undertake such a study for the public and private sector.

A number of departments and agencies opposed the provision in S. 3418 limiting the use of the Social Security number. These included the Commerce Department, Civil Service Commission, Defense Department and the Securities and Exchange Commission. All cited the need for use of the number as an identifier to achieve administrative ends, and the inordinate and prohibitive costs of reprogramming with an alternative number. Numerous private business, banks and industries uniformly opposed this section.

Computer and data professionals from State and local government also opposed the provision, testifying that such prohibitions on its use "would impose a tremendous financial burden on the States and an alternate identifier would have to be developed."

Mailing Lists

The bill now prohibits Federal agencies from selling or renting mailing lists except as authorized by law, but does not require names and addresses to be kept confidential, thus allowing inspection where these are public records. It requires private organizations maintaining a mailing list to remove the individual's name upon request.

A major avenue by which personal privacy and confidentiality may be invaded is the practice of the Federal Government of selling and renting names, addresses and personal data in their files for use in commercial and other mailing lists. Such practices may cause a violation of the tacit or formal agreement by which the agency collected or acquired the information for its own authorized purposes. Laws promoting open records in government have resulted or may result in administrative contracts on agreements to sell the data in bulk, either as a convenience to commercial or other users, or to publicize and promote the purposes of the agency.

While a few examples might be found in which the sale or rental of mailing lists by Federal agencies without specific statutory authority serves a useful purpose, the Committee concludes for several reasons that such action is totally inconsistent with the purposes of the bill as amended. One of these purposes is to entitle an individual to a large measure of control over who, outside of a Federal agency maintaining information about him, has access to his personal information. Mailing lists constitute such personal information when, for example, they represent a group of individuals possessing a certain set of characteristics. The disclosure of this personal information can be damaging to the individual. Therefore, section 206(a) of the bill, as amended, prohibits the sale or rental of lists of names and addresses by Federal agencies unless the sale or rental is specifically authorized by law.

Legislation on this subject has been offered for a number of years. These problems are addressed in S. 3116, introduced by Senator Hatfield and pending before the Constitutional Rights Subcommittee.

Senator Hatfield stated "the real thrust of S. 3116 is not what is received in one's mailbox but privacy and the question of individuals' right to control what is known about them."

He cited the stockpiling of personal information in the businesses who compile and sell lists and other data for commercial purposes. Primarily, this means selling or renting lists to the direct mail industry.

The Committee was told that "lists for this industry are compiled from every imaginable source—telephone, books, magazine subscription lists, credit card lists, church rosters, club memberships, government agencies, newspaper, announcement of birth, death, graduation and from seemingly, inviolate sources such as doctors, dentists, and schools. This flourishing business exists largely without the knowledge of the people who are providing the profit, the people whose names and personal data keep this wheel turning."

Testimony from the Direct Mail Marketing Association shows that it is their recommended practice to remove a person's name from their list if requested to do so. However, only some people know about this service, and the distribution of information through lists is so widespread that people who do manage to get off lists through such a service, have no way of controlling what all the other companies do.

The bill now requires no more of the private sector than that an organization engaged in business in interstate commerce shall remove the individual's name from a mailing list, upon request. Where lists are maintained by private companies, the Committee believes that the decision as to who should be allowed to rent or buy them is a decision best left up to each individual business. However, where such lists are maintained by government agencies, or where names and addresses are sold or rented, the Committee firmly believes that the decision must not be left to individual agency administrators.

Subsection 206(b) requires all persons or organizations engaged in interstate commerce to comply with the written request of an individual who wishes to have his name and address removed from their lists that are used for direct mail solicitation.

This provision represents a sound business practice which is followed by many of the largest and most respectable direct mailers in the country. The Direct Mail Marketing Association, which represents several thousand users of direct mail marketing and advertising in America, has stated in writing to the Senate Government Operations Committee that its Mail Preference Service is specifically designed to permit an individual to have his name removed from its members' lists upon request.

The Committee has been advised by representatives of the Direct Mail Marketing Association and by numerous prominent direct mailers that this practice creates more profitable lists by allowing for the removal of names of individuals who are unlikely to purchase goods or services from the soliciting organization.

The purpose of this provision is to extend this practice to all organizations and to expand the protection to all individuals. It is consistent with the best practice in American industry and with the programs and standards of the Association representing those companies with direct interest in this problem.

The Committee believes such a requirement is a simple and fair one which will not necessitate a revision of private business procedures. Mail order businesses may continue to compile mailing lists and solicit through the mail. The widespread sentiment on this subject for action was noted by Congressman Frank Horton, sponsor of House bill, H.R. 3995, who reported 65 House members sponsoring the bill, 34 Republicans and 31 Democrats.

A survey of mailing list practices of Federal departments and agencies made by the Congressman and another by the House Government Operations Subcommittee chaired by Congressman Moorhead, were offered by Congressman Horton for the hearing record.

The threat to individual privacy from the selling and renting of names and personal information from government files and the use of mailing lists by the mailing list industry was found to be an appropriate subject for privacy legislation by the National Academy of Sciences Project Report. The Committee agrees with the report that the standard of the Direct Mail Marketing Association, mere removal of one's name, is not enough for Government agencies. As the Academy report states, "For many people, this does not resolve the basic privacy issue: when individuals give information about themselves to government agencies for one purpose, usually under legal compulsion to report, should their names, addresses, and data about their occupations, ownership, military service, or other activities be made available to organizations that would use the information for purposes that these individuals consider intrusive?

"In time of major problems of housing, education, crime, race relations, pollution, and peace, it may seem a disturbingly trivial matter to worry about government records leading to the receipt of mail advertisements that some individuals do not want. But the issue symbolizes something we cannot afford to ignore—how do we make the individual's informed consent a more respected and controlling feature in organizational society? Our approach to this problem should not be to make matters confidential which have long been considered open for public access; rather, it should be to find a way to accommodate those who feel their privacy is intruded upon by such direct mail practices. (Report, p. 385)"

Section-by-Section Analysis

TITLE I—PRIVACY PROTECTION COMMISSION

Section 101

ESTABLISHMENT OF COMMISSION

Title I establishes a Federal Privacy Commission, an independent body which the Committee deems absolutely essential to aid in the administrative and enforcement of the act, and to conduct a study of other private and governmental information systems.

Section 101 provides that the five full-time members of the Commission would be appointed by the President subject to confirmation by the Senate. In order to assure the kind of expertise necessary for dealing with the legal, political, social and technological aspects, a commissioner should be considered for selection in part by reason of

his knowledge in one or several of the areas of civil rights and liberties, law, social sciences, computer technology, business, and State and local government. Not more than three of the members of the Commission shall be from the same political party. Commissioners shall serve for terms of three years and for no more than two terms. The President shall select the Chairman of the Commission from its members and he shall be the official spokesman of the Commission in its relations with Congress, the Federal Government and the general public. In this capacity, the Chairman would be expressing the view of the entire Commission. Of course, this would not prevent any other Commissioner from speaking his views, testifying, or providing information to Congress, the Executive or the public. In all other respects, the Chairman shall have equal responsibility and authority in all decisions and actions of the Commission with other members and each member shall have one vote on the Commission.

Section 102

PERSONNEL OF THE COMMISSION

Section 102 authorizes the Commission to appoint an Executive Director and other officers and employees and prescribe their functions and duties. The Executive Director will be compensated at a rate not in excess of the maximum for a GS–18 Federal employee.

In addition to its own employees, the Commission may contract for the services of experts and consultants to carry out its responsibilities. Where these are technicians charged with the inspection of physical and technical security of arrangements, computer equipment and systems, they should be bonded in cases where this is found appropriate.

Section 103

FUNCTIONS OF THE COMMISSION

One of the principal reasons for establishing a Privacy Protection Commission was to fill the present vacuum in the administrative process for overseeing establishment of governmental data banks and personal information systems and examining invasions of individual privacy.

Subsection 103(a)(1). Requires the Commission to publish, and supplement annually, a United States Directory of Information Systems. Each agency is required under subsection 201(e) to notify the Commission of the existence and character of each existing system or file which it maintains on individuals, or any significant expansion or modification of the system. The Commission is directed to publish this information in the Directory of Information Systems together with a listing of all statutes which require the collection of such information by a Federal agency. This is to carry out one of the fundamental principles of the Act that the existence of Federal personal record-keeping systems should not be kept secret from the Congress, the press, or the public. In particular, it is designed to give the citizen one set of accessible documents and one central location where one may reasonably be expected to find out just what agencies are likely to have a file on one and what they are likely to have done with it.

It also provides a published standard for testing and evaluating Federal collection, use and disclosure of personal information in the hands of government. The Committee considers this requirement a substitute for the original requirement of notice to everyone on whom any Federal agency maintains a file, a notice ideally designed to promote the concept of substantive due process throughout government. However, consideration of testimony from experts and of agency objections concerning costs and administrative feasibility of such a requirement resulted in its deletion and replacement by the function of the Commission in this section.

Subsection 103(a)(2). Authorizes the Commissioners to investigate and hold hearings on reports received of violations of the Act. No adjudicatory powers are vested with the Commission and enforcement of the Act rests with the Federal courts. If the Commissioners determine that a violation has occurred, they may report that violation to the President, to the Attorney General, to the Congress, to the General Services Administration where the duties of that agency are involved, and to the Comptroller General if it deems it appropriate for any auditing functions of that agency. S. 3418, as originally introduced, would have given the Commission the power to issue cease and desist orders to stop violations of the Act. The Committee decided, however, to provide for general enforcement of the Act's safeguards, and for the implementation of the exemption provisions, through the administrative channels of each agency, with ultimate review of any challenges in a United States District Court.

Subsection 103(a)(3). MODEL GUIDELINES. The Commission has not been given the power to issue rules and regulations that would b binding on other Federal agencies. However, it is directed to develop model guidelines for implementing the provisions of the Act with interagency consultation and the assistance of appropriate experts in special subject areas. The Committee would expect that other Federal agencies would look to these guidelines before adopting their own rules and their procedures by which individuals could exercise their rights under this legislation.

The Commission is further directed to assist Federal agencies in preparing regulations to meet the technical and administrative requirements of this Act. It is expected that the Commission will retain or contract for expert assistance in information management and technology and other fields in order to provide resources that may not be available to each agency.

Subsection 103(b). Requires the Commission to review, and report on proposed data banks and substantial alteration of existing ones. For this reason, subsection 201(g) requires that Federal agencies report to the Commission on proposals to establish data banks and personal information systems, to significantly expand existing data banks and information systems, to integrate files or establish programs for records linkage within or among agencies, or to centralize resources and facilities for data processing.

The review anticipated here is for several purposes. The Commission is directed to review these reports in order to assess the potential impact of any such proposal on the privacy, due process, and other personal or property rights of individuals or on the confidentiality of personal information. This would include the physical,

technical and administrative security of the data bank or computerized information system. The Committee acknowledges that there are many definitions of privacy and that there is no one precise definition as it relates to the exercise by an individual of rights guaranteed to him under the Constitution or of his right to own and possess property. Each amendment to the Constitution carries with it guarantees against governmental invasions of a particular aspect of individual privacy. Until the concept of privacy can be defined with more precision, the Committee believes that there is a need to study any threatened invasion of a broad range of individual rights by Federal information activities or practices.

In testimony before the Committee on Government Operations and before other committees of the Senate, questions have been raised about the impact of Federal information systems on State programs and powers as well as on the separation of powers existing between the judicial, executive and legislative branches of the Federal Government. Any proposal to establish or alter an information system should be examined in light of its potential to affect the Federal system: to take power or responsibility from the States or to grant responsibilities which should properly be carried out by a Federal agency.

Similarly, any major proposal to expand or create new information-handling technology by Federal agencies for personal data should pose questions for the Commission to attempt to answer regarding the ability of the three branches of government to discharge their responsibilities under such a new system. It is for all of these reasons that agencies must describe in their notices the following matters, under subsection 201(g):

> (1) the effects of such proposals on the rights, benefits, and privileges of the individuals on whom personal information is maintained;
>
> (2) the software and hardware features which would be required to protect security of the system or file and confidentiality of information;
>
> (3) the steps taken by the agency to acquire such features in their systems, including description of consultations with representatives of the National Bureau of Standards and other computer experts; and
>
> (4) a description of changes in existing interagency or intergovernmental relationships in matters involving the collection, processing, sharing, exchange, and dissemination of personal information.

Based upon its review of these proposals, the Commission should submit any findings and recommendations regarding the need for new legislation or administrative action to control or regulate new information-gathering techniques and technology to the President, the Congress, and the General Services Administration.

Subsection 103(c). The Commission is directed to report to the Congress the failure of any proposed data bank or information system to comply with the purposes, standards and safeguards of the Act. In most cases, a review by the Commission of proposals to establish or expand information systems should take no longer than sixty (60) days and should afford the agency sufficient opportunity to alter its proposal if a question regarding compliance with this Act is raised.

This estimate of time is predicated on the full and prompt disclosure to the Commission of agency proposals sufficiently in advance of a final policy decision by the agency to proceed with the proposal to permit adequate review by the Commission. If it is necessary for the Commission to report a failure to comply with the Act, the agency proposing an information system change shall not proceed with this proposal until sixty (60) days after receiving that notification. This is to afford the Congress and responsible executive branch officials an opportunity to act on the agency proposal. If the Commission does not make a determination that the Act has not been violated by an agency proposal, this should not constitute an endorsement of or approval of any invasion of privacy which might result from the implementation of the newer alternate information system.

In carrying out its functions under the Act, the Commission is encouraged to consult to the fullest extent practicable the heads of departments, agencies and instrumentalities of the Federal Government, of State and local governments and of private businesses and other organizations which may be affected by S. 3418. In order to carry out the duties assigned by the Congress, the Commission must be provided access and the opportunity to personally inspect a wide range of confidential material, information maintained by public agencies and private organizations and businesses. In performing its functions the Commission has the difficult task of balancing its need for information with the rights of privacy of citizens. It may, for example, be necessary for it to examine the actual contents and use of certain files held by agencies. Obviously, the Commission itself is bound by the requirements of the Act, including civil and criminal liability for any improper use or divulgence of information it receives in carrying out its responsibilities. The Committee expects the Commission to perform its tasks comprehensively, but has guarded against the creation of an Information Czar. The Commission is not intended to maintain its own files on individuals, or to retain any such personal information in its own possession. The Committee regards this legislation as a means to guard against the integration of separate files on citizens into complete dossiers. The Commission's powers should not be used to frustrate this purpose. In addition, there is no intent to require a national depository for the technical and commercial, and trade documents, or the programming secrets of government organizations and the private sector.

Subsection 103 (d)(1). Mutual cooperation will be important to the successful completion of the study of information systems and the implementation of the safeguards by the agencies covered by the Act. With regard to the Federal Government, the Commission may wish to form an interagency council to work to implement the provisions of the Act.

It is expected that the Commission will also serve as a clearinghouse for various Federal agencies and others to share information on methods of dealing with problems in administering the Act as well as assisting in the exchange of administrative and technological material related to handling of personal information.

Subsection 103(d)(2). It is probable that the Commission will need to study and initiate research projects to determine the best procedures for agency implementation and enforcement of this Act. Because of the highly technical nature of information in system management, re-

search efforts may also be directed toward developing procedures for guarding against unauthorized access to information systems and procedures for implementing the standards and safeguards provided by title to this Act. Where these have already been undertaken by the National Bureau of Standards and other Federal offices, the Commission should take appropriate advantage of those resources to prevent duplication of efforts and to aid in the coordination of Federal efforts in this area.

Subsection 103(d)(3). The Committee added to the functions of the Commission the duty to determine, in connection with its research activities, what specific categories of information should be prohibited by statute from collection by Federal agencies on the basis that the collection of such information would violate an individual's right of privacy.

Section 104

CONFIDENTIALITY OF INFORMATION

In order to fulfill its obligations properly under this Act, the Commission must have access to all data, reports, and other information requested of any department, agency or instrumentality of the executive branch as well as of any independent agency.

Since this will require access to classified documents and other highly sensitive personal information, the Commission may accept identifiable personal data only if it is necessary to carry out its powers and functions. It is directed to establish safeguards to insure that the confidentiality of the information is maintained and upon completion of the purpose for which the information is required it must be destroyed or returned to the agency or person from whom it was received. Because of the strict penalties provided for the unauthorized disclosure of information entrusted to its care, the Committee believes it would be appropriate for the Commission to assure that its technicians and any other employees are bonded before they are permitted access to sensitive information. In addition Commission employees or contractors should be extended the same privileges and be subject to the same requirements for security clearances under the Federal Security Clearance as employees of the agency who have access to the information in question. Under no circumstances should the Commission or its employees be used by another agency for unlawfully obtaining information to which that agency would not be otherwise entitled. The internal rules and regulations of the operation of the Commission should reflect the need for careful handling of this information.

Section 105

POWERS OF THE COMMISSION

The Committee is determined that the Privacy Protection Commission must have certain powers to fully implement a study of personal information systems and to conduct oversight of the proper implementation of the Act in the Federal Government.

In order to investigate reported violations of the Act, the Commission may find it necessary to hold hearings and take testimony as well as receive evidence related to such violations before making any report to the Congress or to the Attorney General. In order to obtain

sufficient information for these hearings or to assemble material for the study of information systems, the Commission is authorized to require by subpoena the attendance of witnesses and the production of books, records, papers, correspondence and documents as it deems advisable.

It is hoped that the Commission would be able to work out voluntary agreements with both public agencies and private organizations for obtaining any material necessary to carry out its statutory responsibilities. Should efforts at voluntary cooperation fail, however, the Committee believes that the role of the Commission is important enough to merit the force of law behind its requests. Under any circumstances, however, no subpoena shall be issued without a vote of the majority of the Commission. The Commission shall appear in court in its own name to enforce subpoenas issued pursuant to this Act, and it shall be represented by attorneys of its own choosing.

Testimony presented before this and other committees, as well as in noncongressional studies, has shown the need and value of the on-site inspection to ensure that regulations adopted pursuant to the Act are in fact adhered to by agencies in their normal day-to-day operations. By giving the Commission the power to take such other actions as may be necessary to implement the Act, the Committee has adopted this recommendation.

While criminal penalties for the violation of this Act are limited to the failure by an officer or employee of a Federal agency to disclose the existence of an information system or the unauthorized disclosure of certain sensitive personal information by a member or employee of the Commission, the Committee felt it was necessary to provide immunity from punishment under this Act pursuant to the provisions of Section 6001(1) of Title 18 of the U.S. Code. This "whistle-blowing section" would permit the Commission to recommend to the Attorney General that a person not be prosecuted under this Act. And this section is designed to encourage the reporting of violations in order to further strengthen the reporting of violations in order to further strengthen the oversight responsibility of the Commission.

The section would authorize the Commission to adopt interpretative rules for the implementation of the rights, standards and safeguards provided by this Act. This is to assure that the rulemaking authority of the Commission is limited to the promulgation of rules and regulations governing its own operations, organization and personnel. This section was included to insure that the courts would not interpret these model guidelines or other rules which the Commission is authorized to issue as having the force of law with respect to any other Federal agency. Rather, such guidelines shall offer only the Commission's best judgment regarding the possible implementation of its safeguards under the Act, and shall serve as a reference only for other Federal agencies to consider in adopting their own rules and regulations.

Section 106

COMMISSION STUDY OF OTHER GOVERNMENTAL AND PRIVATE ORGANIZATION

Section 106 requires the Privacy Commission to make and report on a study of the data banks, automated data processing programs, and information systems of the private sector as well as of regional and

other governmental agencies. As discussed in this report, the decision to authorize such a study is based on the Committee deferral at this time of legislation for abuses of privacy, due process, and confidentiality in the private sector, a need particularly urgent with the growth of national data banks, application of computer technology, and use of new information management practices.

The lack of adequate empirical and legal research to support needed legislation is expected to be remedied by the Commission study and its specific recommendations as to application of the principles or guarantees of this legislation to particular sectors or subject areas, or to particular information linkages between private, State, and Federal data systems. It is further authorized to make such other legislative recommendations as it may determine necessary to protect individual privacy while meeting the legitimate needs of government and society for information. Such study may, on the basis of the Commission's research, take into account the testimony on the original bill advocating regulatory oversight by the Commission or some other Federal agency of all major data banks and information systems affecting privacy.

The Committee found a particular need for examination of the laws and practices governing the kinds of information held by private information collectors which the Federal Government obtains by various means. This includes bank, health, educational, and employment records. It was partly for this reason that the Committee adopted an amendment authorizing the Commission to study what personal information the Federal Government should collect. Congressional studies revealed that most departments and agencies had little cogent knowledge on the extent of their data collection from the private sector and how their demands or their grants, contracts or agreements ultimately affected the privacy of the individual.

Despite some efforts by government and private bodies to study certain aspects of public and private information practices and computer technology, no Federal body has yet been given a broad mandate to examine the status of privacy in both the public and private sector and to recommend specific legislative or administrative action to enhance its protection. Indeed, the President's Domestic Council Committee on Privacy, established in early 1974, immediately perceived the need for a comprehensive survey and analysis of existing and planned data banks and of the laws pertaining to privacy, confidentiality and security. That Committee realized, however, that such a task would be time-consuming and difficult. It relied, therefore, on a recent survey of Federal data banks conducted by a congressional committee. The Privacy Committee of the Secretary of Health, Education, and Welfare had a similar experience. Similarly, a number of Department heads in recent years have discovered that they lacked concrete and comprehensive information about their own agency's systems. Since existing executive offices have neither the authority nor the practical ability and resources to perform such functions, the Committee decided that it was necessary to create the Privacy Commission and charge it with these tasks. In doing so, the Committee has adopted a recommendation made by numerous experts and study panels for almost a decade.

The Commission is directed to complete the privacy study not later than three years from the date of its organization. It is authorized to make periodic reports of its findings to the President and to the

Congress, which will allow it to submit reports and specific recommendations on subject areas as they are completed, and not all at once at the end of its term.

The reports shall include recommendations for applying the requirements and principles of the act to the information practices of organizations under study, whether by legislation, administrative action or by voluntary adoption of those requirements and principles.

Need for Study

Governors and other State and local officials have cited the dearth of information about the practices of regional or national data banks which, because of their interstate nature, are difficult to analyze or control by State privacy laws and regulations. It is thus expected that the Commission's studies, especially those aspects analyzed by States, will assist the States in their own efforts to protect personal privacy.

Representatives of private industries, businesses and organizations have also indicated that such a study would better enable them to meet their ethical and legal obligations to protect individual privacy in an information-rich society while taking full advantage of the benefits of computer technology.

Guidelines for Study

The Committee is aware of the range of possible areas for investigation and of means of conducting such study. Therefore, subsection (b) establishes restraints, limitations and certain research guidelines for the Commission study so that the final product in each case may be responsive to the particular legislative and administrative needs of Congress, the executive branch and agencies of State and local governments.

As a specific requirement, the Committee is to examine and analyze the interstate transfer of information about individuals whether by manual or electronic means. As an example, interstate corporations and multi-state governmental units and private regional data banks exchange among themselves a wide variety of information about people for the purpose of approving credit applications, hiring personnel, examining claims for insurance, and other transactions affecting decisions about the rights, privileges or benefits of individuals. A second example would be the experimental Electronic Funds Transfer System now being developed under the auspices of the Department of the Treasury and the Social Security Administration to electronically transfer social security benefits and other welfare payments from government to bank.

The Commission study is by no means directed to all data banks on people or all personal information systems. Rather, the Commission is charged to study only those which significantly or substantially affect the privacy and other personal and property rights of citizens. The Committee has heard and reviewed much testimony which indicates that interstate and national information networks affect the lives and substantive rights of individuals in a variety of ways. The Committee believes that the Commission should focus its attention on the affects of the collection, use, storage and transfer of information on the rights of individuals.

Social Security Numbers

Particular practices and subjects which the Committee has found are of special concern to the public are designated to be given priority. The Commission is required to study the use of social security numbers, license plate numbers, universal identifiers, and other symbols used to identify individuals in information systems and to gain access to integrate or centralize systems and files. One of the most important problems that has arisen in the Committee's consideration of privacy legislation is the built-in potential among personal information systems for the creation of a national data bank. A single national system utilizing information gathered about individuals from many sources could be advanced by the use of a common identifying number or symbol unique to each individual. The Committee intends that the Commission examine the use of social security numbers and other similar identifying symbols or codes in light of their possible use as universal identifiers, or as indexing tools which may ease the breach of confidentiality or make government record surveillance over the individual easier. The Commission should review laws, regulations and decisions affecting these matters and, in particular, examine the costs and feasibility of halting or restraining present trends in such practices and developing less threatening alternatives in the interest of guaranteeing individual privacy and confidentiality of personal information.

Statistical Data

The Commission is also required to study the matching, integration and analysis of federally produced statistical data with other sources of personal information to reconstruct individual responses to statistical questionnaires for uses other than those for which the information was collected. The Committee was presented with circumstantial evidence in Volume II of the 1971 President's Commission on Federal Statistics which indicates that it is possible, through sophisticated computerized techniques to estimate with reasonable accuracy personal information relating to identifiable individuals using multiple sources of statistical and nonstatistical information published by Federal and State agencies. Such information yields to its user significant information about individuals heretofore held in confidence and thus violating a pledge of confidentiality made by Federal agencies collecting the information for statistical purposes. Commercial firms are rapidly improving this technology, thus creating the need for careful attention to its direction and ultimate capability and its impact on privacy. The Committee intends that particular attention be paid to such developments by certain direct mail marketers, and that the Commission recommend measures to preserve the guarantees of confidentiality provided by existing census statutes and regulations and promised by organizations conducting statistical surveys.

The Committee believes that legislation on privacy issues should give due regard to the preservation of the Federal system and should allow States to provide stronger controls as they see fit or to experiment with their own legislation to meet problems unique in those States. At the same time, they should be afforded all of the information which such a national study can make available. In conducting its study, the Commission is required to examine the laws, Executive

orders, regulations, directives, and judicial decisions which govern the activities under study by the Commission and determine the extent to which they are consistent with the rights of privacy and due process, and other guarantees of the Constitution which this Act seeks to promote. The Committee is cognizant that many laws, regulations and judicial decisions affect the collection of information about individuals and the rights of individual privacy. To fully exercise its study function, the Committee feels that the Privacy Commission should examine these and take them into account as necessary in making its recommendations. In acquiring such information, the Commission may seek the advice and aid of governors, attorneys general, judges, mayors and others with unique control over or knowledge of the public policy and law on privacy matters.

Federal-State Relations

The Commission is directed to determine the extent to which major governmental and private personal information systems affect Federal-State relations or the principle of separation of powers. The Committee believes that many of the personal information systems funded or otherwise sponsored by the Federal Government subtly affect the ways that State governments are able to operate their own information systems and interact with the Federal Government. For one example, a Federal information program that solicits certain types of information about individuals from State governments might also prompt those State governments to begin collecting the same type of information, for their own, perhaps undetermined, uses, without appropriate guarantees of confidentiality. On the other hand, a Federal program may, because of its unforeseen results, be effectively prohibiting the State from adequately promoting the privacy of its citizens, the confidentiality of data about them, or the security of its automated data systems. Where necessary, the Committee intends that the Commission examine the often unforeseen results of Federal-State information-sharing in light of their potential affects on Federal-State relations.

For each matter under study, the Commission is to consider public policy and current standards and criteria governing the collection, soliciting, processing, use, access, integration, dissemination, and transmission of personal information. The Committee heard testimony and has reviewed much material indicating that many information users already impost strict safeguards and confidentiality requirements on their information systems. The Committee wishes the Commission to be able to review these rules and practices in order to determine the scope of their use and their effectiveness as models under particular legislative schemes.

The Commission is also specifically directed to include in its study certain areas which have been shown to be of concern to the public and to legal commentators on privacy issues. These include informational activities in the areas of medicine, education, insurance, employment and personnel, credit, banking and finance, travel, hotel and entertainment reservations, and electronic check processing.

In addition to these, the Commission is authorized to study such other information activities as it believes are necessary to carry out the congressional policy of this Act. This provision is included to

assure that the Commission may be free to examine new developments in means of sophisticated surveillance techniques or of transmitting personal information by satellite and other electronic means.

Exceptions to Committee Study

An exception is made to the Commission's study power for information systems maintained by religious organizations, in order to preserve the principle of separation of church and state. A similar exemption for charitable and political organizations was deleted from the original bill by Committee amendment to assure the broadest scope to the Commission's study for the protection of individual privacy.

This section requires the Commission, to the extent practicable, to collect and utilize findings, reports and research studies of congressional and State committees, other government agencies, private organizations and individuals which pertain to the problems under study by the Commission. The Committee recognizes that there has been much written and said about the issue of personal privacy, due process and confidentiality. In fulfilling its study mandate, the Commission must take full advantage of this research and information. In addition, there are available in computerized form the texts of statutes and judicial opinions.

The Committee expects by this requirement to have incorporated within the Commission study the most valuable aspects of previous research efforts and thereby reduce the administrative costs which a nationwide study might otherwise involve.

In many subject areas, the Commission may need to do no more to meet its obligations on some aspect of the study than develop and draft the specific language for legislative recommendations to be submitted to Congress and the President.

The Commission is also authorized to receive and review individual complaints with respect to any matter under study. This is to assure that wherever possible, the Commission's empirical research shall include, and the recommendations address, the complaints and concerns expressed by individuals or organizations. Frequently, the economic or political consequences of seeking redress from or complaining to the offending agency makes it difficult, if not impossible, for the individual to obtain remedies for invasions of privacy or for wrongs suffered by inaccuracies fed into computerized data systems. The Commission should not have to rely on reports of complaints made to the offending organization.

In addition, in some areas, the lack of sufficient technical and legal resources makes it difficult for Congress to investigate individual cases of information abuses which come to the attention of members to a degree sufficient to produce a record for complex legislation.

As indicated, the Committee does not intend such studies to be theoretical and speculative but to be based on legal research, review of data practices and particular data banks, and investigation of complaints it receives.

SECTION 107

REPORTS

Section 107 provides that the Commission shall, from time to time, and in an annual report, report to the President and the Congress on its activities in carrying out the provisions of this Act.

TITLE II—STANDARDS AND MANAGEMENT SYSTEMS FOR HANDLING INFORMATION RELATING TO INDIVIDUALS

SECTION 201

SAFEGUARD REQUIREMENTS FOR ADMINISTRATIVE, INTELLIGENCE, STATISTICAL-REPORTING, AND RESEARCH PURPOSES

Section 201 sets forth standards and procedures to govern all stages of decision-making for and operation of the information systems of each department and agency of the executive branch.

Subsection 201(a). This subsection is the provision of the bill specifically directed to the constitutional and legal control of the invasion of individual privacy by government. It reflects the intent of the Committee to follow the recommendations of the report of the National Academy of Sciences, that "in terms of privacy there should be a general policy to extend the zones of personal and group freedom from compulsory data collection so that matters that ought not to be considered in making decisions about individuals do not become part of the formal record at all."

Beyond that, this section, together with subsection 201(b)(1) and (7), reflects another dimension of the privacy issue, which is that, under our Constitution, there are, or may be, some human activities of which Government should not take note for any purpose at all because of the detrimental effect on freedom, and that this is true whether or not the information is intended to be used to make decisions about specific individuals.

This section reflects the Committee's effort to insert considerations of privacy in the decision-making process involving management of information systems. As the Academy report states, privacy is "the primary civil liberties issue, since both confidentiality and due process questions disappear if the data are not gathered in the first place, or once they are destroyed."

The section is designed to insure that a Federal agency weighs strongly the rights of personal privacy against its authority and need to gather personal information for a public purpose. Before an information-gathering program may be implemented, the agency must make a determination that its action is authorized and warranted to carry out a statutory obligation. This provision affirms a basic principle of good management in public administration in that it is designed to require that the kind of information about individuals which an agency seeks to gather or solicit, and the criteria for programs to investigate individuals will be, judged by an official at the highest policymaking level to be relevant and necessary to a statutory purpose of the agency.

The section is designed to implement the following policy judgments in the report:

> Not only should the need for and relevance of specific items of personal data have to be established in positive terms but serious consideration should be given to whether some entire record-keeping programs deserve to be continued at all; this was the basic question raised about the Army's domestic intelligence watch over civilian political activity in the late 1960's. A further consideration where need for collecting data

> is at issue is whether records should be retained beyond their period of likely use for the purposes for which they were originally collected.
>
> A related but more complicated question concerns the continued existence of files of information which is no longer supposed to be used for making decisions about individuals. Many cumulative records about individuals in various sectors of the organizational world are filled with facts and evaluations set down in an earlier time, under a different socio-political ethos. In this setting, it is not enough to say "from now on we will not . . ."; steps need to be taken to remove from historical records in high schools, colleges, commercial reporting agencies, law-enforcement files, and other organizations the personal information previously gathered about political, racial, cultural, and sexual matters that would not be put in the files under present rules. To the extent that evaluators today have such records to consult, especially for decisions that are not visible to the individual, the presence of such information represents a dead (and improper) hand from the past.

Most of these provisions contain terminology which will allow administrative definitions to fit particular agency needs and programs. They are intended to be implemented by the model guidelines developed by the Commission which may then be adopted by the agencies or altered as found necessary. This will, for instance, allow for development by Commission experts, in consultation with other Federal officials, of careful, workable definitions of such terms as "accurate," "timely," "complete," and "relevant."

Such a process is also envisioned for determining precise details of the contents of the notices of data banks required to be filed for the Federal Register and with the Commission. These can be discussed and determined with the assistance of the Commission in accordance with an agency's unique problems and record-keeping methods.

Subsection 201(a)(1). Provides that each Federal agency shall collect, solicit and maintain only such personal information as is relevant and necessary to accomplish a statutory purpose of the agency.

This section, therefore, governs the first phase of the process which is the gathering of the information in the first place. The provision reaffirms the basic principles of good management and public administration by assuring that the kinds of information about people which an agency seeks to gather or solicit and the criteria in programs for investigating people are judged by an official at the highest level to be relevant to the needs of the agency as dictated by statute. Second, it requires a decision that the collection of information or investigation of people along certain information lines is necessary in that the needs of the agency and goals of the program cannot reasonably be met through alternative means.

Where there are difficulties in linking a personal data program to statutory authority, it is to be expected that some agencies may face hard decisions of whether or not to seek additional authority, to reject certain programs entirely or to alter investigative standards.

A third element in this decision process is the fact that the information which officials propose to collect must be maintained and

integrated into the agency record-keeping system. Thus the decision on the relevance and need for certain gathering of information and investigating of citizens requires consideration of how that data will overlap or conflict with existing data banks and information programs of the agency.

This section is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary, but rather, must be authorized, and found to be not only reasonable, but warranted by the overriding needs of society as the agency is responsible for administering to those needs.

The provision is the legislative reflection of the conclusion of a panel of the Committee on Scientific and Technical Information of the Federal Science Council which recommended that "an agency should formulate as precisely as possible the policy objectives to be served by a data-gathering activity before it is undertaken. Agencies are encouraged to think carefully about the legitimacy of the activity, the significance of the data for the agency's program, the potential burden on the respondents and the possible availability of the data from some other source. This may make it possible to achieve a reduction in the burden being put on citizens and to harmonize governmental questionnaires and surveys. Great care should be exercised in framing information requests to be certain that the desired information is captured initially and that multiple requests for information is captured initially and that multiple requests for information are avoided, and that no more sensitive personal information is collected than necessary."

Subsection 201(a)(2). Provides that each Federal agency shall collect information to the greatest extent practicable directly from the subject where the information may result in adverse determinations about the individual's rights, benefits, and privileges under Federal programs.

This section, as originally introduced, had no qualifications, but reflected the basic principle of fairness recommended by several reports, that where government investigates a person, it should not depend on hearsay or "hide under the eaves", but inquire directly of the individual about matters personal to him or her.

In order to meet agency objections about the needs of certain civil and criminal law enforcement programs requiring intelligence and investigative information to be collected from other sources, the section was limited to instances where the information sought could affect a person's qualifications to be considered by government for employment or other rights, benefits and privileges. This is the minimum standard of fair procedure, although there may be instances where it cannot be observed. It is expected however that these will be kept to a minimum. Cases may arise for instance, where it is not practical (1) for logistical or financial reasons, or (2) for reason of conflicting, more restrictive, statutory requirements which cannot, after consultation with the Commission, be resolved, or (3) where the information is on hand from other disclosures made by the individual and he has specifically consented at the time of disclosure or later to have it used for other or related purposes within the agency or by another agency.

At the same time as it assures accuracy and fairness to data subjects by this provision, the Committee does not wish to defeat the purposes of the Federal Reports Act to promote the efficient, economical exchange and sharing of information; nor does it wish to impose undue burdens on individuals from whom information is solicited. However when the cause of ordinary efficiency and small economies is weighed against the interest of personal privacy and confidentiality of sensitive information, the Committee expects the balance would tilt in favor of the latter. However, the Act looks to a conscientious weighing of the interests by administrators, and to decisions made on the record pursuant to the discretion allowed by this section.

Even where information is acquired from other sources, an agency should, in the interest of the standards of accuracy and efficiency to be promoted under subsection 201(b) make efforts to have it reviewed by the subject individual. For example, by sending him a copy of the information and affording him an opportunity to affirm, deny or explain it. Such review may constitute compliance with subsection 201(a)(2). This section reflects the committee's adoption of the conclusion of the COSATI panel that "Information should not be collected on a hearsay basis or from people who have only a tenuous association with the data subject and therefore are not in a position to report data from a high probability that it will be accurate."

Subsection 201(a)(3). Requires that each Federal agency shall inform any individual requested to disclose personal information for any purpose whether that disclosure is mandatory or voluntary, by what statutory authority it is solicited, what uses the agency will make of it, what penalties and specific consequences for the individual, which are known to the agency, will result from the nondisclosure, and what rules of confidentiality will govern the information.

This requirement, in various forms, has been universally recommended by commentators and government and private groups, the HEW Report, information specialists, congressional witnesses and others, as basic to the protection of the individual from the arbitrary information power of the Federal Government.

The Committee intends it to remedy the many documented complaints from citizens that they were pressured, coerced, or induced by deceptive means into responding to governmental questionnaires seeking highly personal information for administrative programs, or for census and other statistical and research purposes of the Federal agencies; that they were not told and, furthermore, were frequently unable to learn, even with legal assistance, whether compliance was voluntary or mandatory, what statutes authorized it, what penalties attached to nonresponse, or exactly why the Federal Government wanted the information in the first place.

The section anticipates that Federal requests or requirements for personal information henceforth shall be accompanied by written or oral notices presented in obvious or highly visible manner, which use the specific terms "mandatory" or "voluntary" in describing the nature of the individual's desired response, and providing the other requisite information concerning the authority of the agency to conduct the survey, initiate the inquiry, or, in the case of administrative programs, to ask particular questions of the applicant. The Committee believes that an agency should be able to communicate to the individual, without intimidation, whether he is required to comply with

a request for information and what the likely consequences are of his refusal. To further clearify the consequences of these options, the notices should also include an explanation of the limits on the agency's ability to keep information confidential; for example, under compulsory legal process.

The Committee is not impressed with executive branch arguments and those of some information users which hold that such candor on the part of government represents "poor psychology" and will destroy the integrity of statistical surveys and other data programs, or that it will discourage cooperation with official inquiries. The Committee believes, rather, that just the opposite results will be obtained. Furthermore, the spirit of constitutional considerations of due process and self-incrimination should pervade the conduct of such inquiries for administrative, regulatory, or other such governmental data programs.

In defining the purposes of this section, the Committee endorses the recommendations of the HEW report that "the requirement is intended to discourage organizations from probing unnecessarily for details of people's lives under circumstances in which people may be reluctant to refuse to provide the requested data. It is also intended to discourage coercive collection of personal data that are to be used exclusively for statistical reporting and research."

We also endorse the explanation of the COSATI panel of the need for such protections to avoid "the use of coercion or intimidation in the course of gathering information." We agree with the Panel that: "unless disclosure has been made mandatory by Act of Congress, personal information must never be extracted from an individual without securing his informed, express consent * * * In gathering information from individual citizens, Federal agencies have an obligation to disclose to them the purpose for which the information is being collected, to state clearly the use or uses to which it will be put, to identify the governmental and non-governmental individuals and organizations that will be given access to it, and to indicate whether the individual's name will be associated, either directly or indirectly, with the information.

"The type of disclosure is particularly important when the individual's participation in a data-gathering activity is voluntary in character, and is one way of assuring that the voluntary consent of the individual is meaningful. It enables him to evaluate the risk he may be assuming by revealing personal information, and in some cases, permits him to weigh that risk against the advantages of participating in a particular governmental program. It also should contribute to preventing alienation and should encourage participation in the data-gathering process. For the same reasons, it is imperative that the agency's understanding with the individual be honored.

"When an individual is required to furnish information by act of Congress as is true for the decennial census, informed consent of the type described in the preceding paragraph is not necessary. Nonetheless, it is desirable to provide individual respondents with as much information concerning the data activity as possible."

Of particular concern to people subjected to governmental inquiries is the general lack of precise information afforded at the time of collection about the penalties for and consequences of nondisclosure. Where compliance is mandatory or where untrue response is punishable, with

penalties ranging from $100 to $500 to $1,000 and a year in jail, basic due process principles require that the individual be put on notice of such penalties. The same constitutional considerations require that where such penalties accompany demands for personal data, that demand must be based on statutory authorization.

The Committee considers it basic fairness that any agency provide whatever information it has at hand about the immediate consequence of not responding to an inquiry or particular question. While it may usually be convenient to provide this warning on the face of a written inquiry upon initial collection, in some cases, the Committee recognizes that it may be more practical to supply such information promptly at a later time upon request of a data subject who may voice objection or concern about some phase of a written or oral inquiry, or to some particular question. Clearly, the agency cannot be reasonably expected to tell all foreseeable or imaginable consequences of nondisclosure or disclosure. It can however, advise when nondisclosure will preclude any consideration of an applicant for employment, or for a right, benefit or privilege, or when nonresponse may be accorded some weight in official consideration of the application.

To cite one example:

A Federal employee requested to complete a research questionnaire stating which political candidate he or she prefers should be told at the outset that the response is voluntary, that it will not affect employment, and will not go into any government file. However, even such notice will not preclude an employee electing to challenge the inquiry for possible violation of the limitation in subsection 201(b)(7) on inquiries on first amendment activities.

Similarly, couples applying for Federal housing loans have the right to know if they have to answer questions on whether they intend to have children and if they practice birth control, why the agency requires such information and whether or not they lose the chance for the loan if they don't disclose such information.

Subsection 201(b)(1). Requires each Federal agency that maintains an information system or file to insure, that is issue any requisite regulations, and take affirmative administrative action for the purpose of assuring, that personal information maintained in the system or file, or disseminated from it, is to the maximum extent possible, accurate, complete, timely and relevant to the needs of the agency.

This requirement complements that of subsection 201(a)(1) imposing such a duty on agencies and is deemed necessary to the effective exercise of any right of the individual to challenge a record, or a data bank on these grounds through the agency or the courts.

The standard of relevancy is that statutory basis for an information program required by subsection 201(a)(1). The scope of these two sections encompasses all phases of the information system. The standards of relevaney here relate to the constitutionality and legality of the entire information program, as well as, the reasonableness of maintenance or any particular piece of personal information, given the statutory jursidiction of the agency. The standards of accuracy, completeness, and timeliness, as well as relevancy are directed to the quality of the information in an individual's own file. The section thus looks to a double-pronged consideration, first to the authorized needs of the agency, and second, to the scope of the administrative need for information in order to make a decision on that individual.

The condition that such a goal be pursued to the "maximum extent possible" is attached to promote an extra measure of caution and zeal beyond the ordinary standard of care which governs all other information handling. But it is also designed to allow the agency the freedom to determine through its own regulations and directives, as adapted from the Commission model guidelines, what is reasonably "possible" within the limits of the statutory duties placed on the agency, of its resources, of technological feasibility, and of administrative practicality. The Committee recognized, for instance, that it is administratively and logistically impossible to keep current and timely the statistical information maintained for historical and archival purposes. Yet an agency may well question an investigative data bank or file on people which was long ago outdated and is now seldom used, and which services no program or one which is maintained only in case the individuals once again deal with the agency. It is hoped that with the inclusion of such a broadly-termed mandate linked to the right of the individual to challenge, there will begin a long-overdue evaluation of agency program needs for stale, irrelevant, and untimely information.

When combined with the subsection 201(a)(1) duty to confine information gathering to only personal information relevant and necessary to accomplish a statutory purpose, the Committee has provided agencies and the courts with a standard against which the individual may challenge information in a file or data bank.

Subsection 201(b)(2). States that agencies shall require employees to refrain from disclosing records or personal data in them, within the agency other than to officers or employees who have a need for such record or data in the performance of their duties for the agency

This section is designed to prevent the office gossip, interoffice and interbureau leaks of information about persons of interest in the agency or community, or such actions as the publicizing of information of a sensational or salacious nature or of that detrimental to character or reputation.

This would cover such activities as reading results of psychological tests, reporting personal disclosures contained in personnel and medical records, including questionnaires containing personal financial data filed under the ethical conduct programs of the agency.

It is designed to halt the internal blacklisting that frequently goes on in agencies and on Federal installations on persons who do not comply with the organizational norms and standards for some reason, such as not participating in savings bonds drives or charity campaigns; and the listing of results of employee tests or performances;

It is designed to help prevent the easy exchange of data about the same individual between regional managers of different programs within a bureau or department and the consequent informal or inadvertent administrative integration of data for purposes of making a governmental decision about that person. This might be true, for instance, of a farmer who had filed information or been the subject of official inquiry in several agricultural programs in one county.

The section envisions that if an employee dealing with official information about a person is requested to surrender that person's record to someone who clearly has no need for it, he should decline or seek to define the purpose of the requested disclosure. One of the

results of this section may be to promote a sense of ethical obligation on the part of Federal officials and employees to ascertain when improper disclosure of information within the agency may be sought or promoted for personal, political or commercial motives unrelated to the agency's administrative mission.

It is not intended to conflict with other statutes, rules and regulations governing employee conduct or information practices but is meant to implement and reinforce them. The standard of refraining from certain behavior implies, by definition, not indulging in impulses to engage in positive behavior to the contrary, in this case, in not taking positive action or making specific administrative or personal efforts to disclose personal information acquired in the course of one's duties when such disclosure is not required.

Subsection 201(b)(3). Requires any Federal agency that maintains a personal information system or file to maintain a list of all categories of persons, including individuals and agencies authorized to have regular access to personal information in the system or file.

The original bill required Federal agencies to record each and every access to any information system or file. By requiring instead simply a list of the categories of employees and of other agencies and persons who on a regular basis are permitted to examine files within a system of personal information, the bill meets the objections of agencies that a strict accounting of every access was not administratively practicable or feasible in view of the necessary routine in daily access to a file by varous identifiable groups of people and by many employees for purposes of entering or withdrawing information. The problem of requiring identity and purpose of access by reporters and others in the public exercising inspection rights under that and other acts made it more feasible to require a list which would be available to the public and to individuals who are subjects of the files.

Where employees are concerned, the kind of list envisioned would make it possible to identify for any particular day the employees occupying a position and performing duties requiring such access to a particular file or authorized to have such access. Since this is deemed merely good management and responsible personnel practice for all Federal systems and is a practice observed in many agencies anyway, it is not expected to present difficulties in compliance.

With regard to the definition of who are "regular" users beyond the agency, outside of the public and press, the type of regular use envisioned is that such as where, by statute and written agreement for information-sharing among agencies, there is access by terminal for the purpose of implementing such agreement. The Commission, in the course of developing model regulations for guidance of agencies in implementing the Act, will assist in promoting a workable definition of such users by reference to the specific situations presently authorized.

Subsection 201(b)(4). Requires any Federal agency that maintains a personal information system or file to maintain an accurate accounting of the date, nature, and purpose of nonregular access granted to the system, and each disclosure of personal information made to any person outside the agency, or to another agency, including the name and address of the person or other agency to whom disclosure was made or access was granted. An exception is recognized for those accesses and disclosures involved in public inspection or copying

pursuant to law or regulation, which includes the Federal and State open records laws and regulations implementing them.

This section is included as an essential element of the Code of Fair Information Practice and the "Information Bill of Rights" in order to promote the full implementation of the right to seek to obtain a meaningful correction of inaccurate records, not only in the offering agency, but wherever in government and private organizations the inaccurate information may have been transmitted.

The kind of audit and "audit trail" envisioned here is one that makes it technically and administratively possible to audit and inspect the nature and pattern of transfer of personal information whether in manual or computerized form outside the agency system, to be integrated in another agency's system, or to other persons in other agencies of government.

Furthermore, such record of access and disclosure helps assure against administrative departure from the stated uses, access controls, and users required to be filed in the Federal Register and with the Privacy Commission, and to guard against illegal seizures of information. It is designed to make oversight of information practices of government more manageable and efficient.

Subsection 201(b)(5). Requires a Federal agency that maintains a personal information system or file to establish rules of conduct and notify and instruct each person involved in the design, development, operation, or maintenance of the system or file, or in the collection, use, maintenance, or dissemination of information about an individual, of the requirements of this Act, including any rules and procedures adopted pursuant to this Act and the penalties for noncompliance. This notice would include consultants, contractors, and those outside the agency involved in such activities.

This section, another essential element in the Code of Fair Information Practice, merely recognizes principles of good public administration that the most effective hierarchial management of an organization results from informing employees of their responsibilities and how they relate to overall agency obligation and of their duties regarding the information they process and to the techniques, equipment and instruments with which they carry out their assignments.

While most agencies may have ethical conduct rules with respect to the information under the control of civil servants, these do not necessarily always reflect the ever-expanding information needs of government or the increasing mechanization and computerization of government records, with the vast numbers of specialists and technicians brought rapidly into Federal agencies to deal with them. Nor do these codes reflect the developing professional codes of ethical conduct for those involved in application of computer technology and sophisticated information-processing techniques in the public and private sectors. It is expected that the Commission, in drafting its model guidelines, would incorporate these and would encourage their more extensive adoption by agencies in their rules implementing the Act.

This section thus envisions positive action by the agency, beyond mere publication of implementing regulations, to notify people administratively, perhaps by a handbook for which each person is responsible, and by a special session instructing them on changes made in existing programs by the new Act. It is expected they would be in-

formed of administrative sanctions and other penalties applicable by reason of statutes and regulations governing performance and behavior of Federal personnel.

Subsection 201 (b)(6). Requires any Federal agency that maintains an information system or file to establish appropriate administrative and physical safeguards to insure the security of the information system and confidentiality of personal information processed and handled in it and to protect against any reasonably foreseeable or anticipated threats or hazards to their security or integrity which could result in substantial harm, embarassment, inconvenience, or unfairness to any individual on whom personal information is maintained. [The analysis of this subsection is supplemented by that for subsection 201(f).]

Once privacy, confidentiality and due process policy issues have been resolved, the administrative measures and technical features needed to implement those decisions are required to be taken by the agency under this section. These may include, for example, establishing and enforcing rules of access, adding computer software that appropriately screens requests for access and that keeps accurate and complete records of access and disclosure, and installing locks and similar security devices. Many agencies will no doubt find their present measures adequate for many existing systems and files. Others may need supplementary action. All must make such considerations part of their decisions to create new systems and data banks.

The Committee recognizes the variety of technical security needs of the many different agency systems and files containing personal information as well as the cost and range of possible technological methods of meeting those needs. The Committee, therefore, has not required in this subsection or in this Act a general set of specific technical standards for security of systems. Rather, the agency is merely required to establish those administrative and technical safeguards which it determines appropriate and finds technologically feasible for the adequate protection of the confidentiality of the particular information it keeps against purloining, unauthorized access, and political pressures to yield the information improperly to persons with no formal need for it. Once it determines the need for certain physical and technical features for the computerized or mechanized stages of their systems, or for their manual files, agencies would be expected, in compliance with the Act, to seek such features where necessary through the budget process or as alternatives to existing methods.

The Committee is cognizant of the advice of the Director of the National Bureau of Standards Institute for Computer Sciences and Technology, and intends that the term "appropriate safeguards" should incorporate a standard of reasonableness and "refer to those safeguards which represent current state-of-the-art procedures at any given time, despite any weaknesses that may exist in the technology at that time." However, the Committee does not intend to discourage the active pursuit of new and more useful safeguards.

While this interpretation represents a retreat from the absolute requirement of obtaining such technological features, the Committee agrees that given present cost factors and considerations of economy, such an approach suggests that we could look forward to increasingly higher standards of 'reasonableness' as new technologies are further developed to make our systems progressively more secure. But it

would also permit the immediate application of all of these techniques where they can contribute—even in their present form—to better protection of data confidentiality and individual privacy.

The Act thus provides reasonable leeway for agency allotment of resources to implement this subsection. At the agency level, it allows for a certain amount of "risk management" whereby administrators weigh the importance and likelihood of the threats against the availability of security measures and the consideration of cost.

The Act makes the wisdom and legality of these decisions reviewable by the Commission and Congress where they involve major changes in computerization and file management of data on people. It thus makes Congress, with the advice of the Commission, the final arbiter of the decision weighing cost, economy, technological feasibility against privacy and other civil liberties.

The Committee is furthermore aware of the problems of requiring computers dedicated to one use or one sensitive category of information. Further, it agrees with the National Academy of Sciences Report that "it would hardly advance civil liberties in this country, if in the name of protecting confidential files, civilian government agencies and private organizations were to adopt the authoritarian environments and intrusive personnel policies used by defense and intelligence agencies to safeguard their information systems."

The Committee was persuaded on the need for such standards by the testimony of computer experts and by reported cases of file by theft, tapped transmissions and disclosure problems in the use of time-sharing facilities. As the National Academy report recommendation summarizes numerous expert opinions:

> Both managers and policymakers should be aware that the payoff in sensitive personal information to be obtained by insiders violating confidentiality rules and outsiders breaching system security is going to increase in the coming years. More comprehensive information about people will be collected in the kind of large-scale record systems that are growing up, such as the omnibus charge-card systems and national welfare assistance programs. Furthermore, as more organizations make use of the low cost and flexible services that are available in commercial time-sharing facilities, more high-payoff targets such as the membership and contributor lists of various kinds of organizations will be appearing in time-sharing systems, requiring more attention to the security problems in multiple-user commercial facilities than this area has received thus far. (Report, p. 395)

The range of alternatives available to agencies to promote adequate systems security has been described at length for the Committee record and in other congressional hearings. For convenience and expertise, the National Academy of Science report can be cited here as indicative of the Committee judgment that it is not tying the administrative or logistical hands of the executive branch with strict impossible standards, but is leaving it for the agencies and the Federal Government to request needed specific features from manufacturers in the course of the Federal procurement process. The report states:

> What seems clear is that adequate computer technology already exists to provide both the hardware and software protections that are needed to afford effective levels of security for personal data in the kinds of record systems we have been considering. To give several examples of particular relevance to civil liberties issues, much more could be done by computer manufacturers to put record-field access control features into the software operating systems of computer systems, so that users could exercise greater control over the authorization tables that govern access to the data base for each user. Similarly, much more could be done by software developers to provide the programs for real-time monitoring against unusual volumes of use or unusually low yields of 'hits,' in order to warn systems managers about what may be unauthorized uses or improper 'browsing' in sensitive files. (Report, p. 395)

The Committee does not, therefore, mean to relieve any administration officials of responsibility for promoting the purpose of this subsection. We are aware of the availability of administrative and technological means of promoting this purpose, and are mindful, in particular, of Justice Department technical reports by the Project SEARCH Group and reforms effected by law in the computerized information systems of the States of New York, Massachusetts, Minnesota, and others.

The Committee has taken note of laudable activities in the executive branch to foster administrative observance of standards of confidentiality of information and systems security. Such efforts and management guidelines have heretofore been dependent upon the good will of officials of the department and agencies and upon their zeal, time and discretion in use of resources. This Act will not impede these efforts, but will provide the needed legal support to aid in their achievement.

Subsection 201(b)(7). Provides that no Federal agency that maintains a personal information system or file shall establish any program for the purpose of collecting or maintaining information describing how individuals exercise rights guaranteed by the first amendment unless the head of the agency specifically determines that such program is required for the administration of a statute which the agency is charged with administering or implementing.

This section combined with the application of the principles of relevancy under subsection 201(a), reflects the preferred status which the Committee intends managers of information technology to accord to information touching areas protected by the First Amendment of the Constitution. It is aimed at protecting Americans in the enjoyment of the privacy of their thoughts, habits, attitudes and beliefs in matters having nothing to do with the requirements of their dealings with an agency seeking information. It is designed to assure that where such investigations are undertaken, the decision is made by a responsible official who is accountable on the record rather than by the culminative ad hoc, case-by-case decisions of investigators and drafters of questionnaires which can easily become the common law of an agency's practice in lieu of agency-level decisions.

This section is directed to the planning stage of any executive branch programs being designed for the principal purpose of identifying Americans who exercise their rights under the First Amendment and of taking note of how and when such activities are exercised. It is directed at programs which would (1) require gathering of such data from other agencies or (2) would require questions to be asked of the subject individual or of others about his or her personal political beliefs and philosophy, about legitimate activities of the individual in participating in community events, in religious practices, in seeking redress of grievances through such methods as signing petitions to be sent to Government agencies, Members of Congress or State legislatures; picketing under lawful circumstances; associating with others of like mind for the purposes of exchanging social, economic or political views; engaging in lawful demonstrations with others of like mind for the purpose of expressing opinions about governmental, social or economic policies; or expressing written or spoken opinions about such matters through the press, including letters to editors and comments on radio and television programs.

This section's restraint is aimed particularly at preventing collection of protected information not immediately needed, about law-abiding Americans, on the off-chance that Government or the particular agency might possibly have to deal with them in the future. This, of course, applies not only to the agency's own programs, but also to its participation in such programs undertaken by other agencies.

It is directed to overly-broad inquiries made in the course of administering programs requiring judgments on individuals for determining employment and other rights, qualifications, benefits, or privileges under Federal statutes.

Next, the section is directed to inquiries made for research or statistical purposes which, even though they may be accompanied by sincere pledges of confidentiality are, by the very fact that government make the inquiry, infringing on zones of personal privacy which should be exempted from unwarranted Federal inquiry.

The initiatives for such programs can be highly visible within an agency. They have come to the attention of Congress in formal regulations, in draft regulations, in informal directives and orders establishing programs or specifying certain criteria for gathering information deemed helpful to an agency. The requirements of this section, then, impose a duty on administrators to review such sensitive information programs at the earliest possible stage for their possible reception by the public and the subject individuals as threats to first amendment principles.

Since agency heads and administrators who may doubt their authority will consult their general counsels and the Attorney General as chief legal officer of the Government, it is expected that this section will impose no onerous burden on decision-makers. It is further expected, however, that not only the rigid letter, but the spirit of the Bill of Rights will prevail in their decisions and that where there is dispute about whether to solicit or try to collect the information, the scale will tilt toward observing the privacy of citizens and toward seeking alternative methods of fulfilling the administrative goals of the Federal Government.

The Committee does not expect that compliance will be met by a one-time administrative finding that an agency requires such information. Instead, there are expected to be specific determinations for new programs or alterations in existing ones, for directives on investigative standards, and for specific inquiries to be included on questionnaires sent for administrative, statistical, or research purposes.

The standards are applicable whether the information is sought for another agency's list, or by means of investigative questionnaire, lie-detector, oath, personality test, or any other similar technique.

Such determination will of necessity require reference to requirements of authorizing program statutes, "housekeeping statutes" of the departments and agencies, and pertinent judicial decisions. At a minimum, it expects that compliance will begin with creation of a special reviewing process for such matters at the highest level in each agency and that efforts would be made to seek to learn reaction to similar programs by Congress, the press and public.

Where authority is found to be lacking to make such inquiries as are deemed necessary for a statutory purpose, nothing prevents a department or agency from proposing to the President and from seeking of Congress legislation granting the requisite authority.

In drawing the particular restrictions on data gathering set forth in this section, the Committee does not intend to preclude future decisions that other types of personal information shall not be collected by Federal agencies.

Notices

Subsection 201(c). Provides for the notices describing the personal information systems and data banks maintained by the departments and agencies of the executive branch.

The provision incorporates the recommended language contained in the draft administration bill, and specific recommendations of the HEW privacy committee. The duties herein are required to enable the privacy commission to carry out its duties, as discussed above, pursuant to subsection 103(a), of publishing the Federal directory of personal information systems and data banks.

It is the Committee's intent to specify separately each matter to be included or considered for inclusion in such notices. The categories, however, are broadly stated to allow agencies to adapt their statements to fit their particular systems and files.

The Committee intends that no agency should be exempt from the requirement to develop such information needed for the required notices and to send it to the Commission. In addition, agencies are required to provide such information for publication in the Federal Register simultaneously when the Act becomes effective. Annually thereafter, they are to supplement such notice or, if there has been no change in their personal information systems or data banks, they should either state this or reissue their previous statement. While such simultaneous action may cause an initial logistics problem, the Committee believes it is necessary if the public notice function and the exercise of the rights which it serves are to be meaningful. Congress has received complaints about the difficulty which organizations and individuals have in keeping track of the scattered, obscurely-worded public notices filed by agencies which may affect privacy and civil liberties. In addition, citizens have complained that regional and

local employees of the agencies do not have available in their offices sufficient information about other data banks, investigative or data-collection programs, or information practices of their departments or agencies.

Since the Federal Register is not always available to the average citizen and since the urgency of a problem might preclude his seeking information from the Commission's guide to data banks, the Committee intends that notices with the requisite information should be available for distribution upon request.

It is expected that the contents of notices filed with the commission would of necessity be more detailed and elaborate than that provided for such agency distribution. Such a document might be abbreviated with an indication of where the individual may seek additional information.

The notice to the Commission should contain a listing of all statutes which require the collection of such personal information by the agency. This is to enable the Commission to carry out its function pursuant to subsection 103(a) to publish such list for each data bank and personal information system. This requirement was included by Committee amendment so that Congress and the public may know whether or not the agencies are collecting the information at the discretion or whim of administrators or if there is some statutory basis for it. This requirement to provide such legal data on a systematic basis will enable Congress, if it so desires, to reexamine or modify such statutory authority. Such information on hand will also assist the Commission in its investigation of the complaints of violations of the Act, and in its study of the practices of State and local and private sector organization in which it is to review the statutes and legal authorities for data programs.

Subsection 201(d). States the basic right of the individual to inspect and correct the personal information which the Government has on record about that person. Its provisions are minimum standards and are not intended to preempt or preclude laws and regulations providing even stronger protections for such rights.

These provisions reflect the cumulative recommendations of many experts in constitutional law and of governmental and private groups studying the issues of privacy and due process over many years. They also take into account experience with access and challenge provisions of the Fair Credit Reporting Act, as well as the many recommendations from the Federal Trade Commission, the public, and Members of Congress for strengthening and clarifying that Act.

As originally introduced, the bill provided that each agency notify all individuals about whom personal information is kept in the organization's files. This provision would most clearly have guaranteed that each individual would know what files of personal information are being kept, and by whom, and for what purposes. However, the Committee recognizes the merit of the objection raised by Federal agencies that individual notification would be unjustifiably costly. The Committee relies instead on the initiative of concerned individuals to learn whether they are the subject of government files. Using the Directory of Information Systems as a guide, any individual that writes a letter to any department or agency or official of the Federal Government asking to know what files exist on him shall receive a full

accounting, on behalf of the addressed department or agency and all of its subsidairy governmental organizations, grantees and contractors, of precisely what files do exist.

Subsection 201(d)(1). Requires each Federal agency which maintains an information system or file to assure that an individual who requests them may exercise rights set forth under this subsection. This requirement of "assurance" means no more nor less than that an agency must (1) issue appropriate implementing regulations and (2) take affirmative actions to apply them.

First, the person has the right to be informed of the existence of personal information on him or her, to know whether or not the agency even has a separate file.

In addition, full access to that file is to be afforded and the right to inspect it in a form which is comprehensible. This means that, unlike the existing practice in some agencies and under the Fair Credit Reporting Act, a person does not have to rely on a clerk's review of the file and a summary of what is in it. In addition, an agency may not just present a punched card or a collection of symbols on a print-out from a computerized system, or shorthand notes, but rather, must see that the information is presented in a form which the layman may reasonably understand.

The Committee agrees with the definition of "inspection" provided by numerous reports on privacy and summarized by the Academy of Sciences Report in the following terms:

> . . . where government files are concerned, we think inspection should mean the right of the individual to see a copy or display of the actual record in full, and to obtain an official copy of it for a nominal fee. Having an official describe the contents of the record to the individual but not let him examine it himself does not meet the test of openness or provide the psychological sense of having satisfied oneself about what is really there. (Report, p. 370)

The person is entitled to know the names of all recipients of personal information about such individual, including the recipient organizations and their formal or informal relationship to the system or file, and the purpose and date when the information was given out. This requirement would not apply, of course, where the accounting of access and disclosure under subsection 201(b)(4) need not be maintained because of the exemptions provided in subsection 202(b). It would involve allowing the individual to examine whatever access log is maintained for the file, together with a list of organizations exempted from entry in any log.

The individual also has the right to know the sources of the personal information. If such source is required to be kept confidential by statute, then the individual may be informed only of the nature of the sources.

The data subject may be accompanied by someone of his choice, in order to have the support or advice of a friend, relative, or attorney, in inspecting and evaluating the information and making his way through what may amount to a paper maze. The Committee believes this is necessary for effective exercise of rights under the Act. In some cases, the data may be so derogatory or otherwise sensitive from a privacy standpoint that the individual may be asked to furnish

written permission authorizing discussion of the file in that person's presence.

The person has the right to obtain the disclosures and access required to be given under the Act in person with proper identification, or by mail upon written request. An agency may set reasonable standard charges for document duplication.

This section provides the further right to be completely informed about the uses and disclosure the agency has made of the information so that the individual may trace and correct the further uses of any inaccurate information, or take any necessary action to retrieve it from improper disclosure. The degree of "completeness," of course, would depend on what information the operative official has to his knowledge, or can reasonably obtain. In addition, the handling of such cases would be governed by the agency regulations defining what is deemed complete, timely and relevant to the agency needs in using the information for any purpose.

Subsection 201(d)(2). Describes the actions required of an agency as a minimum response to a person who lets the agency know in some oral or written fashion that he or she wishes to challenge, correct or explain personal information about that person contained in a system or file. Some statutory requirements or regulations may provide greater rights. These procedural rights are recognized as minimum in the recommendations of major commentators and studies. All of them are directed to implementing the basic principles of privacy and due process; that a Government agency should not take note of personal matters at all, and that it should, on the other hand, have information which is accurate and relevant as needed to make fair administrative decisions.

Subsection 201(d)(2)(A). The agency is to investigate the alleged inaccuracy by any reasonable means available and to record the current status of the personal information. Such investigation may require no more than a telephone call to another agency to ask them to verify the data. It may require no more than a review and recording of documentation, affidavits, authoritative materials, or records supplied by the individual. It may mean no more than checking other records and questioning investigators of the agency to clarify vague reports or correct inaccuracies. It may mean no more than reviewing the actions of a computer programmer who deleted or reduced to a minor role relevant information necessary to present a complete and fair account of a situation.

The agency regulations, with the guidance of the Commission's guidelines will provide standards for this and other actions of the reviewing official. The subsection is not intended to require an agency to extend its investigative powers beyond its statutory jurisdiction or beyond the reach of its fiscal and administrative resources. Rather, one of the purposes is to provide fairness to the agency by assuring that administrative means are afforded which allow the agency to protect itself from charges of inaccuracy and untimeliness by taking the necessary action to verify and update the challenged information.

Subsection 201(d)(2)(B). Requires the agency to correct or eliminate any challenged information that its investigation shows to be incomplete, inaccurate, not relevant to its statutory needs, not timely or necessary to be retained, or which can no longer be verified.

The finding of a need for retention can include the uses required by the agency's needs for meeting administrative, research or statistical obligations. The deciding officer should be able to do more than cite a presumed need; rather, the officer should be able to cite a statutory or other legal requirement supporting the decision.

Subsection 201(d)(2)(C). If the investigation does not resolve the dispute, the agency, under this subsection is to accept and include in the record of such information, a statement of reasonable length provided by the data subject setting forth his or her position on the dispute.

Wherever possible, such supplemental information is to be included or entered in the original file. In some cases, where computer programming already undertaken prevents the entry of such disputed information, it may be necessary to store it in a separate file, with an appropriate entry in the formal record of the existence elsewhere of relevant information.

Subsection 201(d)(2)(D). Requires the agency to report the challenged information and to supply the supplemental statement in any subsequent dissemination or use of the disputed information.

Following correction or elimination of challenged data, the agency shall, at the request of the individual, inform previous recipients of its elimination or correction. This requirement is not considered an unreasonable one since the data is conditioned and limited by the informed request of the individual who will have some knowledge of previous recipients and present users from exercising his right to know such matters under subsection (d)(1), and from inspecting whatever monitoring the agency is required to maintain under subsection 201(b) (3) and (4). In addition, the responsible agency officials will have discussed with the person the uses to which the data has been put, to their knowledge, and given him reliable advice on the need for pursuing the corrections with another agency or person. The provision is intended further to reduce the time and resources the individual must expend in correcting his records with each user, office, bureau or agency which may have received it. It will prevent the repetition of the access and challenge efforts for the same purpose.

No time limit was set on the provision, since it may be important to learn if one user received the data under some joint program ten years previous, while those disclosures made in the two years previous may be of no consequence. The deciding official should make some effort within an agency to trace formal or informal programs for exchanging or sharing data which would reasonably involve disclosures from the individual's file for any purpose.

Where such information would not be required to be kept before this Act or would not be kept under the exemptions of this Act, it would recognizably be impossible or difficult to comply with such requirements. In such cases, what is envisioned is a good faith effort to assist the individual.

Subsection 201(d)(2)(F). Establishes machinery for appealing and reviewing the failure to resolve a dispute or the decision of an official to deny a request to correct or supplement information.

Many scholarly proposals to afford the right of access and challenge of records have incorporated such a right within an administrative scheme giving the individual the right to appeal to an independent regulatory body. This was the intent of the original bill which gave

the individual the right to file a statement and provided appeal rights to the Federal Privacy Board, which had cease and desist powers.

The Committee, after considering testimony on the wisdom of alternative methods of regulation, decided against making the new Commission a Federal "ombudsman" complaint body, although it may now receive complaints illustrating patterns of violations of the Act.

Instead, the individual may seek review within the agency and direct judicial review by the Federal District Court in the event the agency rejects the challenge to its records.

At the request of the individual, the agency must provide a hearing within 30 days of the request and the individual may appear with counsel, present evidence and examine and cross-examine witnesses.

If, after such a hearing, the challenged record is found inadequate under 201(d)(2) then the agency must purge it from the file and from the agency system, or modify it as found appropriate.

The actions or inactions of any agency on a request to review and challenge personal data in its possession is made reviewable by the appropriate United States District Court by subsection 201(d)(2)(F)(iii).

The language of this subsection reflects that in an administration-sponsored omnibus criminal justice bill and was recommended by several witnesses and legal experts.

It is the Committee intent to substitute for regulatory agency review, a responsive speedy, agency process for resolving citizen's complaints about improper, illegal, or careless information practices of the Federal Government. Where many agencies may provide a review process after a harmful decision is made with the information, this section anticipates special initiative by agencies to extend existing processes, or to establish new procedures to encompass requests for access and challenge at an earlier stage in the management of the information.

As discussed previously, the Committee deems such access and challenge rights essential to enforcement of the Act, and as an aid to monitoring the system, and to promoting the reduction in the bulk of outdated, irrelevant files which agencies keep.

While agencies may exempt themselves through a rulemaking process, in certain areas, and with respect to particular records, the Committee does not consider the grant of such discretion a mandate to exercise it to the limit, but rather, to exercise it sparingly, with due regard for the principle of democratic government and the recognized right of all citizens to knowledge about the activities of government, a right more precious when the activities relate to information uniquely pertaining to the citizen.

Subsection 201(e). Provides for the coverage of the Act to apply to certain information systems or files of contractors and grantees or others when a Federal agency provides by a contract, grant or agreement for the specific creation or substantial alteration of such information system when the primary purpose of the grant, contract or agreement is the creation or substantial alteration of such an information system.

When such conditions apply, the agency shall, consistent with its authority, cause the requirements of subsections 201 (a), (b), (c), or (d) to be applied to such system and then only to the relevant portions

of such systems or data banks as are specifically created or substantially altered by such grant, contract or agreement.

In cases when contractors and grantees or parties to an agreement are public agencies of State and local governments, the requirements of subsections (a), (b), (c) and (d) shall be deemed to have been met if the Federal agency determines that the State or political subdivisions of the States have adopted legislation or regulations which impose similar or stronger requirements for the security of information systems and the confidentiality of personal information contained therein, and for the individual's right to have access to records and to challenge their accuracy.

Subsection 201(f)(1). This subsection is intended to assure knowledge by Congress, the executive branch, and interested groups of new Federal data banks and pooling of informational and computer resources to constitute centralized data systems not foreseen by Congress. It is to prevent a de facto national data banks on individuals free of the restraints on Federal power established by Constitution and statutes.

It is intended further to prevent creation of data banks and new personal information systems without statutory authorization from Congress and without proper regard for privacy of the individual, confidentiality of data, and security of the system.

The section therefore requires any Federal agency to report to the Commission, the General Services Administration, and to Congress on proposed personal data banks and information systems or files, on proposed significant expansion of existing ones, on integration of major files, on programs for significant records linkage within or among agencies, or for centralization of resources and facilities for automated data processing.

Explanation of this subsection should be supplemented by reference to the analysis of subsections 103(c) and 201(b)(6).

Such notices shall also describe the agency's judgment, positive or negative, of any effect it perceives that such proposal might have on the rights, benefits, and privileges under Government programs of the people who are the subjects of information involved in the change. For instance, does it mean that another agency which makes decisions on other rights of a person will now have terminal access to data of an agency for purposes of making its decisions and thus raise due process issues of relevancy? Will it allow creation of a data bank for investigative or intelligence, or research purposes which might, by its very existence, have an intimidating effect and raise first amendment questions of records surveillance? Will common storage facilities by agencies enable common usage not envisioned by the data subject or facilitate theft or improper access? On the other hand will the changes promote more effective exercise of individual rights, and fairness in decisions about the person?

What is anticipated is a check-off by the agency on the possible enhancement of or threat to the civil liberties and civil rights of citizens, including due process rights, from such changes.

The notice shall also state what administrative and technological features and measures are deemed necessary to protect the security of the information system or data bank and the confidentiality of the information. Such a statement should represent the ideal situation given the kinds of personal information and the promise of confi-

dentiality accorded it by law or by understanding with the subject individual. The report would then include the agency's best judgment on how best to achieve these goals within the limits of available technology, resources, and legislative authority. The subsection requires a description of the formal and informal actions, negotiations, and representations and their outcome, undertaken to obtain necessary features. This should include accounting of any consultation with computer and system experts, including the agency's own staff members and those employed by the National Bureau of Standards, the General Services Administration, by computer manufacturers, and professional organizations on computer and information technology; and any others within and without the executive branch, such as specialists in public administration and constitutional law.

The Committee recognizes that no level of security can be specified as absolutely adequate and that this often depends on what is available to promote the type of security needed for certain types of information.

It is expected that a set of criteria on the degree of sensitivity of personal data in the system would be developed on the basis of the historical breaches of confidentiality of that type of information. It is clear from the various public records and studies that there are some information systems in which there have been breaches for personal gain or political motives or other unauthorized purposes. There is clearly a need to safeguard these files as a first priority. The report to be filed with the Commission would detail the agency plan, given the historical threats or the likelihood of them. Clearly, the files in the Social Security Administration, while sensitive, might not have the same level of possible security breaches as the Passport Office Lookout File or the Civil Service Commission Investigative Index. Attached to that report would be the description of the agency's consultations with the National Bureau of Standards including any recommendations made by Bureau officials and other computer experts on desirable standards for safeguarding information.

Some unnecessary concern has been expressed by certain agencies as to how soon they would have to install such safeguards and whether they would be able to function at all after enactment of the bill until they obtained such features in their systems. For some files or systems, it would be appropriate to define stages and goals to achieve the full level of security. Good-faith compliance can be done in a stage process where necessary, but it is expected that there would be a program of steady and consistent efforts to attain the desired standards.

From the available studies, and from the reports of unauthorized access, it is apparent that few Federal data banks and information systems are living up to existing standards. Testimony to the Committee, the National Academy report and others have shown that there are well-known techniques for controlling authorization of people to use data, to monitor inquiries into the data system, to do current monitoring of the level of use of any participant to detect unusual and possibly unauthorized activity, and other audit-trail techniques. These are all available methods of providing security of systems for administrative, technical, and physical purposes. These and many other techniques are what agencies should be expected to apply to their own situations, within the framework of the Commission model guidelines.

Many of the techniques involved in administrative and physical security would apply to tape central records rooms such as the card index of the Civil Service Commission, the manual fingerprint file of the FBI, and the U.S. Army Records Center.

However, computer systems pose special problems because of on-line terminal communications. Therefore, the growth useful standards and procedure could be nourished.

The notice should include a description of changes in existing inter-agency or intergovernmental informational relationships, whether these are pursuant to Executive order, statute, agreement, or custom. This is to afford the Commission, interested groups, and the Congress an opportunity to evaluate the impact of such computerization or changes in information systems on the observance or principles of separation of powers and of federalism including their impact on powers and authority of State and local governments.

It is expected that precise details to be included in such reports may be arranged with the Privacy Commission, pursuant to consideration of logistical and administrative feasibility.

The Committee intends, by requiring the filing of such notices and the Commission review of them, to assure to the extent possible under this Act the promotion of the public policy reflected in the National Academy of Sciences report that: "All aspects of important new record systems should be subject to examination as to their civil liberties implications and as to citizen reaction to their various features. As with computerization itself, the process of establishing new record systems or changing old ones in executive agencies ought to become more visible and deliberate * * *" (*Report*, p. 399).

Subsection 201(f)(2). Provides that the agency must delay the proposal for 60 days if the Commission, after reviewing the agency's notice and investigating its implications under the terms of the Act and the mandate to the agency under subsection 201(b)(6), as discussed above, notifies the agency that the proposal does not comply with the standards for privacy, confidentiality, and system security established under the Act or by regulation pursuant to it.

This allows the Commission time to file any investigative reports on the matter as required pursuant to title I. Nothing in this Act then prevents agency officials from proceeding with this proposal, nor, on the other hand, does anything in the Act require them to proceed with it. This subsection merely provides for a moratorium of 60 days where the Commission, under its mandate, finds a proposal so fraught with actual or potential constitutional, legal, or administrative difficulties that it ought to be specifically examined or authorized by Congress, or ought to receive the further attention of appropriate high level executive branch officials.

Subsection 201(g). Provides that each Federal agency covered by this Act which maintains a personal information system or file shall make reasonable efforts to serve advance notice on the subject of information before it disseminates or makes available a file or any data on that person pursuant to compulsory legal process. The purpose of this section is to permit an individual advance notice so that he may take appropriate legal steps to suppress a subpoena for his personal data. When it undertakes itself to notify the individual, it may require that the cost burden of such efforts must be borne by the requesting agency or person.

The committee intends subsection (g) to impose stricter requirements upon the disclosure of information to protect it from the searches of random investigators who may obtain information from friendly employees or who may simply flash a badge or use influence to obtain such information. However, the subsection is not intended to require compulsory legal process where it is not presently required. Nor is it intended to loosen any present restrictions imposed by statute or regulation whereby information may only be obtained through court order or other legal process. This subsection reflects the Committee's agreement with the HEW report recommendation which was found necessary "to assure that an individual will know that data are being sought by subpena, summons, or other compulsory legal process, so as to enable the person to assert whatever rights are available to prevent disclosure of the data if such actions seem desirable.

This section is intended to apply to all personal information held by an agency, including administrative, statistical and research data. It is intended to be a separate safeguard independent of any other exemptions in the Act in order to carry out the principle that an individual should be put on notice whenever any agency official is under judicial compulsion to surrender data, and to know whenever personal data will be put to uses unknown to the individual and not specified by the agency in its published notices. In summary, it is designed to assure that the person will be able to exercise rights under this Act to check the data for accuracy or to monitor its further use and redisclosure by the requesting agency or person. Since it is not intended to subtract from existing legal safeguards covering such information demands, it is also intended to allow the individual to exercise any existing rights under Federal and State laws and regulations to challenge the issuance of administrative or judicial orders.

Subsection 201 (h). Provides that no person may condition the granting or withholding of any right, privilege, or benefit, or make as a condition of employment the securing by any individual of any information which may be obtained through the exercise of any right secured under the provisions of section 201. It reflects the committee's intention to protect the data subject from coercion by Government agencies or private businesses and organizations who may condition rights, privileges, benefits or considerations otherwise due the person equally with all other citizens upon the obtaining of a personal file or data. This subsection reflects the concerns of administration and agency spokesmen who feared that opening up the individual's personal files which have been protected from disclosure to that person or to others in society would subject the person to all kinds of demands for medical and other personal records. Since the committee's intent is to make certain inroads into the well-meaning paternalism of Federal agencies so that an individual may be advised what information the agency is collecting or holding, this subsection provides a right against such coercion which is enforceable in the Federal District Court in a civil action pursuant to section 303(c). This subsection is not intended to prevent an individual from seeking and obtaining rights under section 201, but is designed to provide a legal remedy for what are believed to be unreasonable and coercive pressures on that person sufficient to state a cause of action before a Federal judge.

Section 202

DISCLOSURE OF INFORMATION

Subsection 202(a). Provides that no Federal agency shall disclose, transfer or disseminate personal files and information to any person, agency or private organization unless certain conditions are met. In conjunction with subsection 201(a)(3), this section is intended to promote the informed consent of the individual to the uses to which government puts the personal data it collects or creates. It is thus expected to exert some check on excessive or illegal reach of governmental power over the individual, and on illegal or inadvertent centralization of investigative programs and linkage of data Federal banks with those in the State and local governments and the private sector. By allowing the individual to know where the data is flowing, the provision should also assist in preventing the illegal or improper use of data by agency officials and employees who have no business with the file or information.

Subsection 202(a)(1). Requires the agency to make written request to the individual and obtain his or her written consent. Compliance with this safeguard may be at the time of initial collection.

Subsection 202(a)(2). Requires the agency to make no such dissemination unless the recipient of the information has adopted rules in conformity with the Act for maintaining the security of its information systems and files and the confidentiality of the information. This mandate, similar to recommendations of several reports and commentators, is to assure continuance upon transfer to another agency or to a governmental or private organization for a Federal purpose, of the protection to which the information is entitled because of the original understanding with the citizen or the originating agency or organization. It is intended to apply to transfer of a particular file of any individual as well as to the transfer of mass data from one automated information system to another, and to the linkage of information systems. If the formal or informal security procedures of the receiving agency clearly or impliedly would allow the data to be used in ways not intended by the individual and not advanced by the agency in its dealings with the person, then no transfer could be made. This would also apply to intergovernmental data-sharing such as transfer of internal revenue files to State and local governments without assuring proper protection for the confidentiality of the data.

While the original bill and the HEW Report envisioned an agency's determining "substantial" assurance of observance by the other agency of such protections, the Committee was told by computer experts and agency representatives that it would be difficult for one agency to enforce such conditions within another agency. Thus, the subsection requires the agency to look to published rules for its judgment on the wisdom of transfer, but anticipates that compliance with the subsection would usually result in creation of interagency negotiations and a record of formal agreement for the conditions of transfer and for protection of the data in the receiving agency.

Subsection 202(a)(3). Prohibits dissemination unless the information is to be used only for the purposes set forth by the sender or by the recipient pursuant to the requirements for notice under subsection

201(c). Again, the same considerations of enforcement and privacy guarantees applicable to the previous subsection apply to this one. The agency transferring is expected, at the minimum, to protect the individual and the public interest by assuring that the uses for which the new agency or user states that it wishes the data are consistent with those for which formal notice has been given by either the transferring agency or the receiving agency or user. Additional guarantees beyond those of this section may be pursued, and, indeed, are encouraged. The Committee recognizes that some agencies take such further precautions as a matter of course for transfer of personal information. This is particularly true of data transferred pursuant to the Federal personnel security program and Executive orders dealing with classified information. Nothing in this section is intended to reduce the strength of those administrative protections for guarantees of privacy and confidentiality.

Executive branch spokesmen and others have advocated that these conditions for interagency and other types of disclosure should be in the alternative. They believe that mere consent of the individual may be enough, or that notice to the public at large of the agency's intended use, or mere requirement of administrative and technical protections for the information, would each alone be sufficient as the general rule governing transfer of personal data. The Committee has disagreed with this approach in the belief that there may be an aura of compulsion or possible threat of intimidation, or an apparent unfair inducement of the individual attached to a request or requirement to surrender personal information for one governmental purpose. This may amount to improper Federal pressure to consent to any and all uses to which the agency may put the data, including that attendant upon interagency or intergovernmental transfer. The best way of guarding against this kind of implicit governmental pressure and affording the individual adequate protection is to require all three conditions. In addition, this prevents an agency from merely citing a notice of intended "use" as a routine and easy means of justifying transfer or release of information. Administration spokesmen were concerned that this might expand interagency data-swapping. By allowing the agency to cite a "use" disclosed by its published notice, the bill is not intended to broaden dissemination and interagency transfer where they must be pursuant to or are required or limited by over 150 Federal statutes. Since subsection 201(a) requires that personal information collected or maintained by the agency be relevant to a statutory purpose, the notice of use and purpose filed with the Commission for the particular information system or data bank will, of necessity, incorporate those statutory uses, and reliance on that notice for transfer authority would represent compliance with subsection 202(a)(3).

The Committee therefore recognizes the great variety of uncoordinated ad hoc, and sometimes poorly authorized patterns of data transfer among agencies. This section does not require such transfers and sharing among agencies, nor does it preclude the additional requirement of other guarantees for safeguarding the individual as well as the originating agency. It is designed to assure, in the future, that one government agency does not use the personal information given by the individual or by third parties to another agency to make what might be a detrimental decision affecting qualifications, rights, bene-

afforded under existing laws and practices will not be affected by any provisions of this Act. It assures that the General Accounting Office as an arm of Congress will be able to continue to meet its information needs for auditing and inspecting agency programs as required by the Budgeting and Accounting Act and other statutes. This subsection therefore provides that the accounting of access and disclosure required in subsection 201(b)(4) and the conditions which subsection 202(a) attaches to disclosure to other persons and to inter-agency transfer shall not be applied when disclosure would be to the Comptroller General or any of his authorized representatives in the course of the performance of the duties of the General Accounting Office. It affirms that nothing in this Act shall impair access by the Comptroller General or his representatives to records maintained by an agency, including records of personal information, in the course of performance of their duties. This subsection reflects the advice of the Comptroller General that such a provision is needed to protect the existing powers which he exercises on behalf of Congress, but that it will not enhance or detract from such powers.

Subsection 202(e). This subsection is designed to provide a general guide for construing the duty imposed on agencies by this section and those imposed by the Federal Reports Act and other statutes to promote efficiency and economy by combining data requests and sharing the results and thus reduce repetitive demands on citizens. It is to reflect the Committee's intent that the requirements of this section are to be interpreted as a mandate to continue enforcement of the duties imposed by other statutes, and that they should not prevent agencies from taking whatever management steps are needed to implement the two goals in drafting their questionnaires and in planning and carrying out their information programs. In addition, it has been included to meet the concerns of Administration spokesmen that the minimum safeguards for interagency disclosure under this section might be interpreted by agencies as an indication that they could relax their efforts to comply with the present restrictions placed on some exchanges of information between agencies for the purpose of promoting confidentiality of certain kinds of records.

The Committee believes that there are a number of administrative devices for assuring observance of the two sets of values in Federal information programs, but we have not attempted to close all of the administrative loopholes which allow violation of confidentiality.

Subsection 202(f). Provides an exemption from the written request to the individual prerequisite for disclosure with respect to requests by law enforcement agencies. Obviously it would be inappropriate to require a law enforcement agency to get permission of the subject of a criminal history record prior to obtaining a copy from another law enforcement agency. Such a requirement would in effect prohibit the routine exchange of records through the FBI's Identification Division or the National Crime Information Center (NCIC). Likewise, it might frustrate legitimate criminal investigations if a law enforcement agency were required to get permission from the subject of a file maintained by a non-law enforcement agency before the former agency could gain access. (e.g. FBI access to a tax return).

Subsection 202(f). Recognizes both types of law enforcement, disclosure, or access to files by distinguishing between routine and non-routine exchanges of information with law enforcement agencies. The Committee assumes that most routine exchanges with law enforcement agencies involve law enforcement records such as rap sheets or criminal histories and is between two law enforcement agencies; and that the less routine disclosure to a law enforcement agency involves a law enforcement agency request of a non-law enforcement agency. Therefore subsection (e) permits law enforcement disclosure in the former circumstance, where there is a program of routine exchange, if there is a formal agreement between the two agencies respecting such exchange. The subsection permits law enforcement access in the second circumstance, non-routine requests only where written requests and permission are given on a case-by-case basis by the agency maintaining the record. The Committee is of the view that the agency which maintains the records should assure, via the written permission or the formal agreement that the recipient has complied with subsection 202(a)(2) and adopted rules on security, confidentiality, and privacy.

If the exchange is on a routine basis, the two agencies should adopt a formal agreement between themselves setting out which records will be exchanged, how the records may be used and the privacy, confidentiality, and security regulations which the recipient agency has adopted. The sanction for failure to comply with the agreement should be interruption of routine exchange by the maintaining agency. This formal agreement concept is based upon the terminal users agreement now used by NCIC and by state and local law enforcement agencies which operate data banks. The Commission and the Attorney General would, of course, have to determine whether an existing terminal agreement adequately meets the requirements of this subsection once this bill is enacted and how that concept will be applied to manual files. Any such agreements would in effect be public documents since they would be incorporated into the public notice given on the information systems as required by subsection 201(e).

Although the Committee believes that public notice and exposure of such routine exchange will act as a check on abuses of such arrangements, the committee hopes that routine exchange will be restricted to essential law enforcement records such as rap sheets and that those records will only be exchanged by such agreement between law enforcement agencies. All other types of access should be via the written request according to the agency procedure. In requiring that the agency rule on each request on a case-by-case basis, it is hoped that secret law enforcement access, that is disclosure without notification to the subject of the file, will only be permitted in the most exigent and essential circumstances. In each such case, the agency must find that such circumstances exist and that the law enforcement agency has described the information requested in sufficient particularly to meet the requirements of the subsection. The subsection specifically requires that the law enforcement agency set out in its written request of the agency "the particular portion of the information desired and the law enforcement activity for which the information is sought."

SECTION 203

EXEMPTIONS

Subsection 203(a). The Committee believes that it is fundamental to the implementation of any privacy legislation that no system of personal information be operated or maintained in secret by a Federal agency. The existence and certain characteristics of each system should be a matter of public record, and testimony before the Committee has indicated that this information can be made public without compromising critical information used by agencies responsible for the national defense or foreign policy of the country.

The potential for serious damage to the national defense or foreign policy could arise if the notice describing any information system included categories or sources of information required by subsection 201(c)(3)(E) or provided individuals access to files maintained about them as required by subsection 201(a).

The Committee does not by this legislation intend to jeopardize the collection of intelligence information related to national defense or foreign policy, or open to inspection information classified pursuant to Executive Order 11652 to persons who do not have an appropriate security clearance or need to know.

This section is not intended to provide a blanket exemption to all information systems or files maintained by an agency which deal with national defense and foreign policy information. Many personnel files and other systems may not be subject to security classification or may not cause damage to the national defense or foreign policy simply by permitting the subjects of such files to inspect them and seek changes in their contents under this Act. In order to obtain an exemption from subsection 201(c)(3)(E) or 201(d), it must be shown that the application of those subsections would damage or impede the purpose for which the information is maintained.

Subsection 203(b). Exempts from full compliance with the access and challenge provisions of section 201 and the disclosure provisions of section 202, that information which an agency head determines is investigative information or law enforcement intelligence information. Both terms are precisely defined in the definitions section of the bill contained in Title III. All of these definitions are based in large part on the criminal justice privacy bills (S. 2963 and S. 2964) discussed earlier in the section of the report dealing with law enforcement.

The effect of this subsection is to require the agency head to determine first what portion of files maintained in any information system in his agency or which his agency might fund on the State or local level contains information which falls within the definitions—"Investigative information" or "law enforcement intelligence information." Investigative information might include information in a file maintained by a legitimate law enforcement agency, defined as an agency which can make an arrest for violation of a Federal or State statute. Investigative information might also be maintained by an agency which is not a law enforcement agency but which is gathering the information in the course of investigating activity which falls within its regulatory jurisdiction. For example, this section would permit the Chairman of the SEC to exempt from access and challenge files maintained by his agency on individuals whom it is investigating for violation of the SEC laws.

The exemption for intelligence information is restricted for the most part to law enforcement agencies. It was the Committee's view that there were no regulatory or non-law enforcement agencies which had a legitimate right to maintain intelligence files and that therefore none of their investigative files should be exempt from the access, challenge and disclosure provisions via reliance on exemptions for intelligence information.

Once the agency head determines that he has information legitimately in one of his information systems which falls within these definitions then he must, via the rulemaking process, determine that application of the challenge, access and disclosure provisions would "seriously damage or impede the purpose for which the information is maintained". The Committee intends that this public rulemaking process would involve candid discussion of the general type of information that the agency maintains which it feels falls within these definitions and the reasons why access, challenge or disclosure would "seriously damage" the purpose of the maintenance of the information. The Committee hastens to point out that even if the agency head can legitimately make such a finding he can only exempt the information itself or classes of such information (e.g. all wiretap transcripts maintained at FBI) and not a whole filing system simply because intelligence or investigative information is commingled with information and files which should be legitimately subject to the access, challenge and disclosure provisions.

The subsection 203 (b) qualifies the exemption from access and disclosure for investigative information in two important respects. First, investigative information may not be exempted under this section where the information is maintained longer than is necessary to commence criminal prosecution. This qualification recognizes the amendments to the Freedom of Information Act recently adopted by the Senate (the so-called Hart amendment). Second, the subsection states that the Act is not intended to disturb the rules of criminal and civil discovery of investigative files presently permitted by the Federal Rules of Criminal and Civil Discovery and, other State or Federal court rules, administrative regulations or statutes such as the so-called "Jencks" statute (18 USC 3500).

Subsection 203 (c)(1). The head of any agency may determine that an information system file or personal information maintained by that agency qualifies for an exemption under subsection (a) or (b) of this section. To secure the exemption, a notice of proposed rule-making must be published in the Federal Register at least 30 days prior to holding rule-making proceedings and provide a copy of that notice to the Privacy Protection Commission to afford the Commission the opportunity to comment. Where possible, agencies are encouraged to provide up to 60 days' notice of hearings to afford all interested parties an opportunity to comment or appear.

The notice of the proposed rule-making shall conform to the requirements of sections 553(b), (c) and (e); 556, and 557 of Title 5, United States Code and shall include a specification of the nature and purpose of the system file or information to be exempted as provided by subsection 201(c) of this Act.

After the period of notice, the agency shall give interested persons an opportunity to participate in the rule-making through submission of written arguments or through oral presentation at a public hearing.

After consideration of the relevant matter presented, the agency shall incorporate in the rules adopted a concise general statement of their basis and purpose.

SECTION 204

ARCHIVAL RECORDS

Subsection 204(a). Provides for certain applications of the Act to archival records. Federal agency records which are deposited and accepted by the Administrator of General Services for storage, processing and servicing in accordance with section 3103 of title 44 of the United States Code are to be considered as though maintained by the agency which deposited the records and subject to all of the provisions of this Act, where they apply to such agency records. The Administrator of General Services is prohibited from disclosing such records or any information in them, except to the agency which maintains the records or pursuant to the rules established by that agency.

Subsection 204(b). Provides that Federal agency records pertaining to identifiable individuals which were transferred to the National Archives of the United States as records which have sufficient historical or other value to warrant their continued preservation by the Federal Government are to be considered to be maintained by the National Archives for the purposes of this Act. Except for the required annual public notice set forth in subsection 201(c), the only provisions for the act which shall apply to such records are subsections 201(b)(5), requiring the establishment of rules of conduct and appropriate training for employees and 201(b)(6), requiring the establishment of appropriate administrative, technical and physical safeguards to protect the confidentiality of personal information. These provisions are, to a large extent, already a part of existing rules of the National Archives and hence should pose no unwarranted administrative burden.The Committee finds no reason why the Administrator should not establish rules of conduct and notify the employees and others involved in any phase of the information system or file of the requirements of the Act concerning the need for respect for the needs of privacy, confidentiality and for security of the system. In addition, there is no valid reason why the Archives should be exempt from the requirement to establish the appropriate safeguards to insure the security of the system.

Along with all other agencies, the National Archives is subject to the notice requirements of the bill.

Subsection 204(c). Provides that the National Archives shall notify the Commission and give public notice of the existence and character of the personal information systems and files which it maintains for its own internal uses and for other purposes and cause such notice to be published in the Federal Register. While it realizes the difficulties of describing these precisely, the Committee intends such notice to include at least the information specified by subsection 201(c)(3) (G), (I) and (J).

The Administrator of the General Services Administration testified against application of the bill to records under GSA control or to those in the National Archives. This is particularly true of the Archives.

records which are generally over 50 years old and are not well organized. The Committee consulted with GSA staff and has learned that records at the Archives are inadequately indexed and involve large volumes of data in more than 20,000 separate filing systems; hence the Committee believes that the administrative cost of compliance by the Archives would far outweigh any potential benefits, particularly since records cannot be disclosed by the Archives unless they are at least 50 years old. However, the Committee intends that the Administrator of General Services take special precautions to ensure that records older than 50 years not be disclosed when disclosure is likely to cause discreditation or injury to an elderly individual or the living relatives of deceased individuals. In the case of Bureau of the Census records assembled subsequent to the year 1900, disclosure ought to be subject to the approval of the Secretary of Commerce.

The Committee believes that this section adequately meets the problems he described in his testimony. It is designed to further the interest of historians and others in preserving the integrity of historical records and in promoting access to them, within the constraints of the needs for individual privacy, for confidentiality and due process of law.

Section 205

EXCEPTIONS

Section 205 provides certain general exceptions and clarifies legislative intent.

Subsection 205(a). Shows the Committee's intent that the exemptions provided in the Freedom of Information Act to the required disclosure of Federal information on certain subjects, and that permitted for protection of personal privacy may not be used as authority to deny an individual personal information otherwise available under this Act.

Subsection 205(b). Reflects the Committee's intent that the Act does not affect existing requirements to disclose, disseminate, or publish information which an agency is required to collect for the purpose of making such disclosure. This subsection was included at the request of the Securities and Exchange Commission and other regulatory agencies to assure that this Act will not affect their statutory duties to publish information.

Subsection 205(c). Exempts from the access and challenge provisions information collected, furnished or used by the Census Bureau for statistical purposes or as authorized by the Federal Census statutes. While statistical records are subject to other safeguards and requirements of the Act, the Committee believes that the complex statutory and administrative scheme presently governing census and statistical information needs careful legislative review before attempting to apply the provisions for access, challenge and review of such records. The Director of the Census Bureau referred to the millions of statistical records now in existence and the very specific procedures and rigorous safeguards applied to them. The Census Bureau records are not used to make decisions about individuals but are used to furnish to those individuals extracts of otherwise confidential information about themselves, and their immediate families.

SECTION 206

MAILING LISTS

Subsection 206(a). Prohibits, unless specifically authorized by law, the practice by Federal departments and agencies of selling or renting names and addresses which they acquire during their transactions with individuals or which they obtain through their dealings with other agencies. The Committee believes this provision is consistent with the intent of the bill to prevent disclosures of personal information without consent or specific authority. As discussed in this report the clear difficulty in obtaining consent free of the appearance of intimidation and the impossibility of assuring limited use once the data is sold or rented, makes it advisable to require specific approval by Congress when the agency undertakes to sell or rent this data in bulk.

This stipulation should not be construed to require an agency to withhold from the public names and addresses which are otherwise permitted to be made public.

The provision is not intended to affect the protection already afforded and the authorized uses now designated for the names and addresses of individual postal customers maintained by the Postal Service to facilitate mail delivery, mail forwarding, and address and mailing list correction services. Present law prohibits the Postal Service from making available to the public any mailing or other list of names and addresses, except as specifically provided by law.

Subsection 206(b). Deals with the disclosure and use of names and addresses by any person, including businesses and organizations, engaged in interstate commerce, who maintains a mailing list. It requires removal of the individual's name and address from such list, upon written request of that individual. The bill thus provides a right to individuals which heretofore has been granted by some organizations, and which has been recognized by the Direct Mail Marketing Association as a desirable standard for organizations which use mailing lists. This provision does not attempt to regulate the maintenance of files and personal records of State and local governments, or of organizations or their use of names and address for communicating with customers, clients and others with whom they have commercial transactions or official business.

TITLE III—MISCELLANEOUS

Section 301

DEFINITIONS

Section 301 contains the definitions applicable to the bill.

The Committee has used the term *"personal information"* throughout the bill to mean any information about the individual that identifies or describes any characteristic including but not limited to education, financial transactions, medical history, criminal or employment record, or any personal information that affords a basis for inferring personal characteristics such as finger and voice prints, photographs, or things done by or to such individual. Such definition

includes the record or present registration, or membership in an organization or activity, or admission to an institution. It is intended to include within these terms any symbol, number, such as a social security number or character, address, by which the individual is indexed in a file or retrievable from it.

The reference to personal characteristics does not exclude a file that contains only names and is headed by a general label for a category of records. If the heading or the nature of the file represents a judgment on the individual or a subjective view, then that file would be subject to the bill. A file headed "security risks" or one labeled "malingerers," or one coded for people to be dismissed at the earliest opportunity, even if the file only contained names, would be covered. This could, for instance, include a list of people who do not buy bonds, or do not contribute to charitable causes. Thus it could cover a list which contained names only but which, by its nature, conveyed something detrimental or threatening to the reputation, rights, benefits or privileges or qualification of the individual simply by reason of being listed on it. There are many data banks and files with names maintained strictly for housekeeping purposes, and it is expected that the Commission model guidelines will make some distinctions for the degrees of sensitivity of such files, and will allow for the development of special treatment for files where the potential for abuse and harm is very great, and those for housekeeping purposes such as who works on a holiday or who has a parking space.

The term "*individual*" means a citizen of the United States or an alien lawfully admitted through permanent residence. This term is used instead of the term "person" throughout the bill in order to distinguish between the rights which are given to the citizen as an individual under this Act and the rights of proprietorships, businesses and corporations which are not intended to be covered by this Act. This distinction was to insure that the bill leaves untouched the Federal Government's information activities for such purposes as economic regulations. This definition was also included to exempt the coverage of the bill intelligence files and data banks devoted solely to foreign nationals or maintained by the State Department, the Central Intelligence Agency and other agencies for the purpose of dealing with nonresident aliens and people in other countries.

The term "*information system*" was adopted to indicate the application of the bill to all of the components and operations, whether automated or manual or otherwise maintained, by which personal information, including the name or identifier, is collected, stored, processed, handled or disseminated by an agency.

Rather than focus on a single record or subject file, the Committee has adopted an approach focused on the total information system which includes all phases of information collection, storage, handling, processing, dessimination and transfer. It includes records which are computerized, mechanized, microfilmed and photographed. The bill thus is directed to the overall programs and policies of executive branch departments and agencies including the design, development, and management of an information system, as well as to the maintenance of one particular file on an individual, or the gathering of information on one data subject. With such a definition, the duties and responsibilities imposed by the bill apply to administrators, computer

programmers and all manner of employees including technicians, clerks, guards. Given the broad scope of the bill, an alternative use of the term "system of record" would create confusion as to its possible application to such things as inventories and extraneous matters.

The use of the terms "information system" and "files" allows for distinctions where needed for the application of certain standards to an entire information system of an agency, department, or establishment, including its bureaus, offices, employees, and equipment, and for the application of them to a particular file, that is, a series of records, on a particular subject.

The terms *"file"* and *"data bank"* in public usage are frequently interchangeable.

Under this bill, "file" may mean an individual record or a series of records containing personal information about individuals which may be maintained within an information system. "Data bank" means a collection of files pertaining to individuals. Used in the bill, it connotes a recognizable entity for management purposes, specifically located within an agency or organization or to one of its components; it means a collection of files usually contributed to by different users and available to them according to a plan of access.

The term *"Federal agency"* means any department, agency, instrumentality, or establishment in the executive branch of the Government of the United States. The definition includes any officer or employee of an agency. In addition to the general purpose of this provision to define the application of the Act, it is also intended that the definition assist in placing the responsibility for intra-agency handling of information on the head of the department or agency.

The term *"investigative information"* has a special and narrow meaning under this bill. It has been discussed at length in the section of the report entitled "Law Enforcement Files". It means information associated with an identifiable individual compiled by—

(1) an agency in the course of conducting a criminal investigation of a specific criminal act where such investigation is pursuant to a statutory function of the agency. Such information may pertain to that criminal act and be derived from reports of informants and investigators, or from any type of surveillance. The term does not include criminal history information nor does it include initial reports filed by a law enforcement agency describing a specific incident, indexed chronologically and expressly required by State or Federal statute to be made public; and

(2) by an agency with regulatory jurisdiction which is not a law enforcement agency in the course of conducting an investigation of specific activity which falls within the agency's regulatory jurisdiction. For the purposes of this paragraph, an "agency with regulatory jurisdiction" is an agency which is empowered to enforce any Federal statute or regulation, the violation of which subjects the violator to criminal or civil penalties.

The term *"law enforcement intelligence information"* means information associated with an identifiable individual compiled by a law enforcement agency in the course of conducting an investigation of an individual in anticipation that he may commit a specific criminal act,

including information derived from reports of informants, investigators, or from any type of surveillance. The term does not include criminal history information nor does it include initial reports filed by a law enforcement agency describing a specific incident, indexed chronologically by incident and expressly required by State or Federal statute to be made public.

The term "*criminal history information*" means information on an individual consisting of notations of arrests, detentions, indictments, informations, or other formal criminal charges and any disposition arising from those arrests, detentions, indictments, informations, or charges. The term shall not include an original book of entry or police blotter maintained by a law enforcement agency at the place of an original arrest or place of detention, indexed chronologically and required to be made public, nor shall it include court records of public criminal proceedings indexed chronologically.

The term "*law enforcement agency*" means an agency whose employees or agents are empowered by State or Federal law to make arrests for violations of State or Federal law.

Section 302

CRIMINAL PENALTY

Section 302 provides for criminal penalties for willful violations of the Act in two respects. One is for the secret creation of data banks in violation of the requirement that all such decisions be made public. Any officer or employee of any Federal agency who willfully keeps an information system without meeting the notice requirements of this Act set forth in subsection 201(c) shall be fined not more than $10,000 in each instance or imprisoned not more than five years, or both.

The other violation subjects an officer or employee of the Commission to criminal penalty for the unlawful disclosure or transfer of personal information about any individual obtained in the course of such officer or employee's duties in any manner or for any purpose not specifically authorized by law and provides that such person be fined not more than $10,000 or imprisoned not more than five years, or both.

These are the only violations of the Act subject to criminal sanction. The Committee has decided to provide criminal sanctions for these two violations because they are key to any effective protection for privacy and confidentiality. The public policy requires that all data banks be subject to a visible public policy decision. The entire Act would be frustrated if secret data banks could be created and operated with impunity. The Committee has underlined this judgment by not permitting an exclusion from this requirement even for those highly sensitive data banks in the areas of national defense, foreign policy or law enforcement. A strongly-enforced requirement of publicity in the creation of data banks is necessary for administrative oversight, legislative oversight, and judicial review.

Equally fundamental is the need to guard against unlawful dissemination, disclosure or transfers of personal information acquired by the Commission consultants and employees in the course of their duties.

While Commission employees are also subject to the same Federal criminal laws and government-wide regulations penalizing all other Federal employees who disclose information, this section creates sanctions uniquely applicable to them. This is deemed necessary since in exercise of its powers and performance of investigative duties, the Commission may obtain or examine all kinds of administrative documents and data relative to executive branch implementation and enforcement of the Act, as well as information on individuals needed to determine violations of the Act. In addition, for purposes of its research and studies, it may engage in similar activities with respect to certain data banks and systems of the private sector and in State and local governments.

In light of such special auditing, inspection and study functions, strong penalties were deemed necessary to reassure government agencies and citizens that the deterrents to improper disclosure are so severe that they need not worry about improper or illegal disclosures.

SECTION 303

CIVIL REMEDIES

Section 303 provides for civil judicial enforcement of the Act by persons affected by violations of the Act. In keeping with general legislative practice, this bill not only establishes certain administrative requirements and grants certain rights to citizens, but gives authority to the citizen to defend his rights by taking the initiative of court action. Such a right is doubly important since the revised bill gives no enforcement authority to the Commission.

Subsection 303(a). Gives a cause of action to a citizen aggrieved by a denial of access to his own file. Since access to a file is the key to insuring the citizen's right of accuracy, completeness, and relevancy, a denial of access affords the citizen the right to raise these issues in court. This would be the means by which a citizen could challenge any exemption from the requirements of sections 201 and 202 made pursuant to the procedures outlined in section 203. A person seeking access to a file which he has reason to believe is being maintained on him for the purposes of determining its accuracy and completeness, for example, or to take advantage of the rights afforded him under section 201, could raise the question of the propriety of the exemption which denies him access to his files. In deciding whether the citizen has a right to see his file or to learn whether the agency has a file on him, the court would of necessity have to decide the legitimacy of the agency's reasons for the denial of access, or refusal of an answer. The Committee intends that any citizen who is denied a right of access under the Act may have a cause of action, without the necessity of having to show that a decision has been made on the basis of it, and without having to show some further injury, such as loss of job or other benefit, that might stem from the denial of access. Since it is often exceedingly difficult for a citizen to learn of such consequences, or if he knows, to establish a "cause and effect" relationship between the information in his file and some subsequent damage to him, the Committee has decided that it would frustrate an individual's ability to assert his rights if he had to allege and prove use or such consequential harm. In order to state a cause of action, it should be enough that he be able to assert that the presumptive right of access granted him by the Act has been denied him.

Subsection 303(b). Affords the Attorney General and any aggrieved person authority to enforce the Act as against existing or threatened violations of the Act by seeking a Federal District Court injunction against such acts or practices. This subsection has a two-fold purpose. First, it gives the Attorney General the obligation to challenge in court any violation of the Act which might affect the public at large, but which does not yet affect any particular citizen sufficiently to give him constitutional standing to sue, or which may not be such as to induce a private person to endure the practical difficulties of litigation.

Second, the grant of a cause of action to any "aggrieved person" is designed to encourage the widest possible citizen enforcement through the judicial process. This is necessary, as mentioned, since the Act does not give any administrative body authority to ensure compliance with the Act. The Committee intends the use of the term "aggrieved person" to afford the widest possible standing consistent with the constitutional requirement of "case or controversy" in Article III, Sec. 2 of the Constitution. In this respect, the provision is designed, among other things, to supply certain deficiencies in standing and ripeness which the courts found in the *Environmental Protection Agency* v. *Mink*, 410 U.S. 73 (1973), *Laird* v. *Tatum* (408 U.S. 1(1972), and *Stark* v. *Schultz*, 42 U.S.L.W. 4481 (Apr. 1, 1974)).

Subsection 303(c). Provides that any person found to have violated provisions of the Act or any rule, regulation, or order issued under it shall be liable to the aggrieved person for actual damages sustained by the individual, punitive damages where appropriate, and in case of successful action, the cost of the action, with reasonable attorney's fees to be determined by the court.

In addition to damages, the aggrieved person would receive the benefit of any other appropriate remedies, including injunctive or mandatory relief, which the court deems appropriate.

The final subsection makes clear that the Federal courts will have jurisdiction regardless of the fact that the amount claimed is less than $10,000.

Section 304

Jurisdiction of district courts

Subsection 304(a). Gives jurisdiction to the Federal courts to hear cases brought under section 303 and to examine information *in camera* to determine whether the information or any part of it may be withheld under any of the exemptions in section 203 of the Act. The agency has the burden of sustaining the legality of its actions. Venue would most likely be either in the plaintiff's jurisdiction, or in Washington, D.C., although other venue is possible. The section also ensures that the court will have the power to examine *in camera* any contested information necessary to a determination of the litigation, thus among other things, remedying the lack of reviewing power which the Supreme Court found in the *Mink* case. Since the burden of justifying the withholding of information is on the agency, this will enable the court to make a full *de novo* determination of the propriety of the grounds asserted by the government for keeping the information from the plaintiff. Such a provision is necessary in order to provide a full and complete hearing to the issues being litigated and to provide justice to the aggrieved individual.

Subsection 304(b). Provides that in any action to obtain judicial review of a decision to exempt any personal information from any provision of this Act, the Court may examine such information *in camera* to determine if all, or any part of it, is properly classified with respect to national defense, foreign policy, or law enforcement intelligence or investigative information and may be exempted from any provision of this Act. The burden is on the Federal agency to sustain any claim that such information may be so exempted.

Section 305

EFFECTIVE DATE

Provides that the Act shall become effective one year after the date of enactment, except that the provisions of title I shall become effective on the date of enactment.

This provision is designed to allow the agencies lead time to develop their regulations and to seek such additional resources or assistance as they may need to meet their obligations under the Act. By allowing the immediate implementation of the provisions establishing the Commission, the Committee intends to permit the Commission time to develop its model guidelines, establish any needed interagency councils, and generally to prepare for full implementation of the Act.

Section 306

AUTHORIZATION OF APPROPRIATIONS

Authorizes appropriation of such sums as may be necessary to carry out the provisions of the Act.

New Title

The title is amended so as to read:

"A bill to establish a Privacy Protection Commission, to provide management systems in Federal agencies and certain other organizations with respect to the gathering and disclosure of information concerning individuals, and for other purposes."

Estimated Cost of the Legislation

The Committee has received a broad variety of generalized statements of the estimated costs of implementing the safeguards and guarantees provided in this legislation. No precise estimate of costs can be established until the Commission develops model guidelines and until the Act is applied to specific information programs and administrators have reviewed their resources for implementing it in accordance with their own rules. The Committee believes that good faith enforcement of the standards and procedures for review will result in substantial savings to Federal agencies. We are mindful, for instance, of testimony describing the Navy's destruction of 15 tons of records upon review of its program needs for retention of records. Similar patterns showed up in the review by the Army of the relevance to its statutory programs to the personal information it collected and maintained on individuals who had no dealings with the armed services.

Since a number of agencies already apply some of the safeguards to certain of their files, and since the Act will require little or no further effort on their part for those files, this certainly will affect the cost of implementation. Furthermore, experience under the practices of those agencies and with provisions which are somewhat similar in the Fair Credit Reporting Act and other statutes shows that the workload is not unreasonable and, in some cases under those laws, did not meet expectations. The very existence of the statutory guarantees apparently tended to reassure citizens that government and organizations were following certain guidelines pursuant to administrative and legislative oversight.

The HEW report addressed the problem of costs and the Committee agrees with the commonsense observations there:

> The safeguards we recommend will not be without costs, which will vary from system to system. The personal data record-keeping practices of some organizations already meet many of the standards called for by the safeguards. . . . We believe that the cost to most organizations of changing their customary practices in order to assure adherence to our recommended safeguards will be higher in management attention and psychic energy than in dollars. These costs can be regarded in part as deferred costs that should already have been incurred to protect personal privacy, and in part as insurance against future problems that may result from adverse effects of automated personal data systems. From a practical point of view, we can expect to reap the full advantages of these systems only if active public antipathy to their use is not provoked. (Report, p. 44, 45)

The Office of Management and Budget has been unable to provide an accurate cost estimate.

ROLLCALL VOTE ON FINAL PASSAGE

In compliance with section 133 of the Legislative Reorganization Act of 1946, as amended, rollcall votes taken during Committee consideration of this legislation are as follows:

FINAL PASSAGE: Ordered reported: 9 yeas—0 nays

Yeas:
Jackson
Muskie
Chiles
Nunn
Huddleston
Percy
Roth
Brock
Ervin

(Proxy)
Ribicoff
Javits.

Nays:
None